

CR-128956

SPACE SHUTTLE SORTIE PAYLOAD CREW SAFETY AND SYSTEMS COMPATIBILITY CRITERIA

(NASA-CR-128956) SPACE SHUTTLE SORTIE
PAYLOAD CREW SAFETY AND SYSTEMS
COMPATIBILITY CRITERIA. VOLUME 2: CREW
SAFETY DESIGN AND VERIFICATION (TRW
Systems Group) 90 p HC \$4.75 CSCL 22B

N75-13017

Unclas
04831

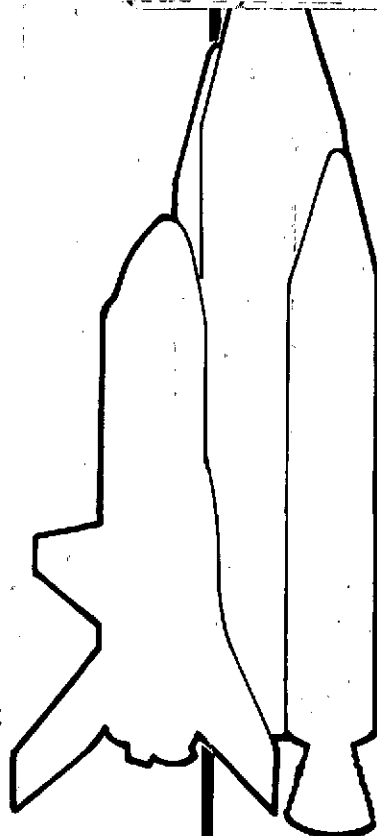
G3/18

Volume II

Crew Safety Design and Verification Criteria

15 MAY 1973

FINAL REPORT



TRW
SYSTEMS GROUP

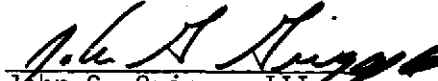
SPACE SHUTTLE SORTIE PAYLOAD
CREW SAFETY AND SYSTEMS COMPATIBILITY CRITERIA

VOLUME II - CREW SAFETY DESIGN AND VERIFICATION CRITERIA


Prepared for
National Aeronautics and Space Administration
Lyndon B. Johnson Space Center
Houston, Texas 77058


Under Contract
NAS9-12742

Prepared by:


John G. Griggs, III
Principal Investigator

Approvals:


Marshall F. Conover
Study Project Manager
Systems Engineering Laboratory
TRW Systems Groups


Earle M. Crum *
Technical Manager
Payloads Engineering Office
NASA/JSC

* Approval is given with respect to complete responsiveness to contractual requirements and does not, at this time, necessarily imply total NASA acceptance of all conclusions contained herein.

TRW
SYSTEMS GROUP

FOREWORD

Space shuttle characteristics are expected to allow selective easing of many cost-inducing criteria now required of payloads placed in orbit by expendable launch systems. Of particular interest is the prerequisite of identifying and differentiating between the minimum, mandatory design and verification criteria for sortie payloads and all other criteria for payload projects.

The TRW Systems Group under two concurrent contracts to NASA/JSC (NAS9-12741 and NAS9-12742) has performed a combined study effort entitled "Space Shuttle Sortie Payload Crew Safety and Systems Compatibility Criteria" for the express purpose of addressing the determination of mandatory and discretionary design and verification criteria applicable to sortie payloads from operational space shuttle management viewpoint. The study projects were performed during the period from 16 May 1972 through 15 May 1973.

The studies were sponsored jointly by NASA Headquarter's Mission and Payload Integration Office of the Office of Manned Space Flight, and the Lyndon B. Johnson Space Center's Engineering and Development Directorate. Study direction was provided by Mr. Earle M. Crum of the Future Programs Division, Payloads Engineering Office. He was assisted by a NASA Management Team representing NASA Headquarters, Johnson Space; Kennedy Space; Langley Research; Lewis Research; and Marshall Space Flight Centers.

The results of these studies are documented in the following three volumes:

Space Shuttle Sortie Payload Crew Safety and Systems
Compatibility Criteria Documentation

<u>Volume</u>	<u>Title</u>	<u>Document No.</u>
I	Executive Summary	22214/22215-H013-R0-00
II	Crew Safety Design and Verification Criteria	22214-H014-R0-00
III	Systems Compatibility Design and Verification Criteria	22215-H014-R0-00

CONTENTS

	Page
1. INTRODUCTION	1-1
1.1 Background	1-1
1.2 Objectives	1-1
1.3 Scope	1-2
2. PRECEDENT PRACTICES RESEARCH	2-1
2.1 Approach	2-1
2.1.1 Required Information	2-1
2.1.2 Programs to be Researched	2-2
2.1.3 Data Search	2-3
2.2 Conclusions	2-4
2.3 Recommendations	2-4
3. CATEGORIZATION PROCESSES DETERMINATION	3-1
3.1 Approach	3-1
3.2 Design Process	3-2
3.3 Verification Process Determination	3-7
4. CANDIDATE CRITERIA DETERMINATION	4-1
4.1 Primary Sources	4-2
4.2 Applicable Hazard Areas	4-3
4.3 Criteria Synthesis	4-3
5. HAZARD ANALYSIS	5-1
5.1 Assumptions and Limitations	5-1
5.2 Generalized Sortie Payload	5-2
5.3 Analysis	5-2
6. CREW SAFETY DESIGN AND VERIFICATION CRITERIA	6-1
6.1 Design Criteria	6-1
6.2 Verification Criteria	6-4
6.3 Criteria Limitations	6-4
6.3.1 Critical	6-4
6.3.2 Ionizing Radiation	6-5
6.4 Subsystems Cross Referencee	6-5
7. CONCLUSIONS	7-1
7.1 Study Results	7-1
7.2 Program Offices	7-1
7.3 Systems Safety Design Criteria Categories	7-1
7.4 Safety Requirements and Guidelines	7-2
7.5 Hardware Safety	7-2
REFERENCES	R-1
BIBLIOGRAPHY	R-2

TABLES

		Page
1-1	Specific Study Objectives	1-2
1-2	Study Guidelines	1-4
2-1	Research Queries Applied to Each Program	2-2
2-2	Conclusions from Precedent Practices Research . .	2-5
2-3	Recommendations from Precedent Practices Research	2-7
5-1	Generalized Sortie Payload Subsystems and Considerations	5-3
5-2	Preliminary Sortie Payload Hazard Analysis . . .	5-4
6-1	Crew Safety Criteria Summary	6-2
6-2	Explosive Device (ED) Criteria	6-6
6-3	Electrical Shock (ES) Criteria	6-9
6-4	Energy Source Isolation (ESI) Criteria	6-10
6-5	EVA/IVA (E/I) Criteria	6-14
6-6	Materials Compatibility (MC) Criteria	6-19
6-7	Ionizing Radiation (IR) Criteria	6-20
6-8	Contamination/Toxicity (C/T) Criteria	6-23
6-9	Fire (F) Criteria	6-25
6-10	Fuels and Oxidizers (F/O) Criteria	6-27
6-11	Pressure Vessel (PV) Criteria	6-28
6-12	Structural (S) Criteria	6-33
6-13	Systems Interactions (SI) Criteria	6-35
6-14	Subsystems Cross Reference	6-36

FIGURES

		Page
1-1	Shuttle Sortie Payload Philosophy	1-3
3-1	Crew Safety Design Categorization Process	3-3
3-2	Verification Process	3-8

NOMENCLATURE

AC	Alternating Current
AFETR	Air Force Eastern Test Range
AFETRM	Air Force Eastern Test Range Manual
AFSC	Air Force Systems Command
AGE	Aerospace Ground Equipment
ARC	Ames Research Center
ATR	Aerospace Technical Report
AVE	Aerospace Vehicle Equipment
CEI	Contractor End Item
c.g.	Center of Gravity
C/T	Contamination/Toxicity
CV	Convair
D	Discretionary
DAC	Douglas Aircraft Company
DC	Direct Current
DH	Design Handbook
DOD	Department of Defense
ECLS	Environment Control and Life Support
ED	Explosive Devices
E/I	EVA/IVA
EMI	Electromagnetic Interference
EPS	Electrical Power System
ERAP	Earth Resources Aircraft Program
EREP	Earth Resources Experiment Package
ES	Electrical Shock
ESI	Energy Source Isolation
EVA	Extravehicular Activity
F	Fire
F/O	Fuels and Oxidizers

NOMENCLATURE (Continued)

g	Gravity
GDCA	General Dynamics Convair Aerospace Division
GE	General Electric Company
GFE	Government Furnished Equipment
G&N	Guidance and Navigation
GOX	Gaseous Oxygen
GSE	Ground Support Equipment
HDBK	Handbook
HEAO	High Energy Astronomical Observatory
Hqtrs	Headquarters (NASA)
IR	Infrared
IR	Ionization Radiation
IVA	Intravehicular Activity
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
KV	Kilovolts
LHe	Liquid Helium
LH ₂	Liquid Hydrogen
LMSC	Lockheed Missiles and Space Company
LNe	Liquid Neon
LN ₂	Liquid Nitrogen
LOX	Liquid Oxygen
M	Mandatory
MC	Materials Compatibility
MIL	Military
MMC	Martin Marietta Corporation
MOL	Manned Orbiting Laboratory
MSC	Manned Spacecraft Center

NOMENCLATURE (Continued)

MSCM	Manned Spacecraft Center Manual
MSFC	Marshall Space Flight Center
MSS	Mission Specialist Station
N_2	Nitrogen
NAS	National Aeronautics and Space
NASA	National Aeronautics and Space Administration
NHB	NASA Handbook
NR	North American Rockwell
O_2	Oxygen
OMSF	Office of Manned Space Flight
PI	Principal Investigator
PSS	Payload Specialist Station
PV	Pressure Vessels
RAM	Research and Applications Modules
R&D	Research and Development
RF	Radio Frequency
R/QA	Reliability/Quality Assurance
RTG	Radioisotope Thermoelectric Generator
S	Structural
SAMSO	Space and Missile Systems Organization
SD	Space Division of Rockwell
SI	Systems Interactions
SP	Special Publications
SPD	Safety Program Directive
STD	Standards

NOMENCLATURE (Concluded)

TBD	To Be Determined
TOR	Technical Operating Report
USAF	United States Air Force
UV	Ultraviolet
°C	Degrees Celsius (Centigrade)
°F	Degrees Fahrenheit

1. INTRODUCTION

1.1 BACKGROUND

NASA is currently examining shuttle payload costs in an effort to both more accurately predict and reduce such costs. History indicates that the criteria applied by NASA to previous space payloads caused them to be quite expensive. This practice was acceptable considering the costs associated with the launch and the necessity for a high probability of mission success. However, when these costs are used to estimate the cost of future shuttle payloads, it is evident that there would soon be a cost factor limiting the use of the shuttle.

Fortunately, the shuttle characteristics will allow selectively easing many of the cost-inducing criteria now placed on expendable launch system payloads. Relaxing these criteria is expected to greatly reduce the cost of space payload development.

Central to those cost-reducing efforts must be the capability to identify and differentiate between the minimum, mandatory design and verification criteria for shuttle sortie payloads and all other candidate criteria for payload projects. Accordingly, this study will contribute to lower sortie payload costs by producing a methodology capable of defining only the minimum criteria required for crew safety from a sortie payload. The resulting criteria will form the basis of future specifications to be developed when quantitative shuttle data are available.

1.2 OBJECTIVES

The prime objective of this study was to identify the minimum, mandatory payload design and verification criteria necessary to insure that sortie payloads are safe with respect to the crew of the space shuttle system, distinguishing them from those criteria related to mission success, configuration choices or management approaches which are, therefore, discretionary to project management as variables in cost/benefit trades. Specific study objectives are tabulated in Table 1-1.

Table 1-1. Specific Study Objectives

- Research, identify, and analyze past safety practices in analogous payload situations to establish a historical perspective and to utilize available experience.
- Establish categorizing processes for distinguishing between shuttle mandatory and discretionary crew safety design and verification criteria.
- Identify the mandatory design and verification criteria that are required by shuttle management to insure crew safety of sortie payloads with the space shuttle system.
- Identify the crew safety design and verification criteria that are discretionary to payload management as variables in cost/benefit trades.

1.3 SCOPE

The scope of this study is bounded by the sortie payload definition illustrated in Figure 1-1. These elements remain attached to the orbiter at all times and therefore do not include propulsion systems nor free-flying satellites. A given sortie payload may interface with the shuttle mission specialist station (MSS) or the payload specialist station (PSS) and excludes a remote manipulator system. Several pallets of experimental equipment may reside in the payload bay as well as piggy-back package(s). Additionally, as in Skylab, some experiment equipments may also be included in the shuttle crew compartments.

Accordingly, the criteria derived by this study are applicable to sortie payload elements carried in the shuttle payload bay or in the crew compartments, and are intended to insure the safety of the crew. Additional criteria which are contained in the systems compatibility report (volume III of this report) reflect control of incompatibilities which could have safety implications.

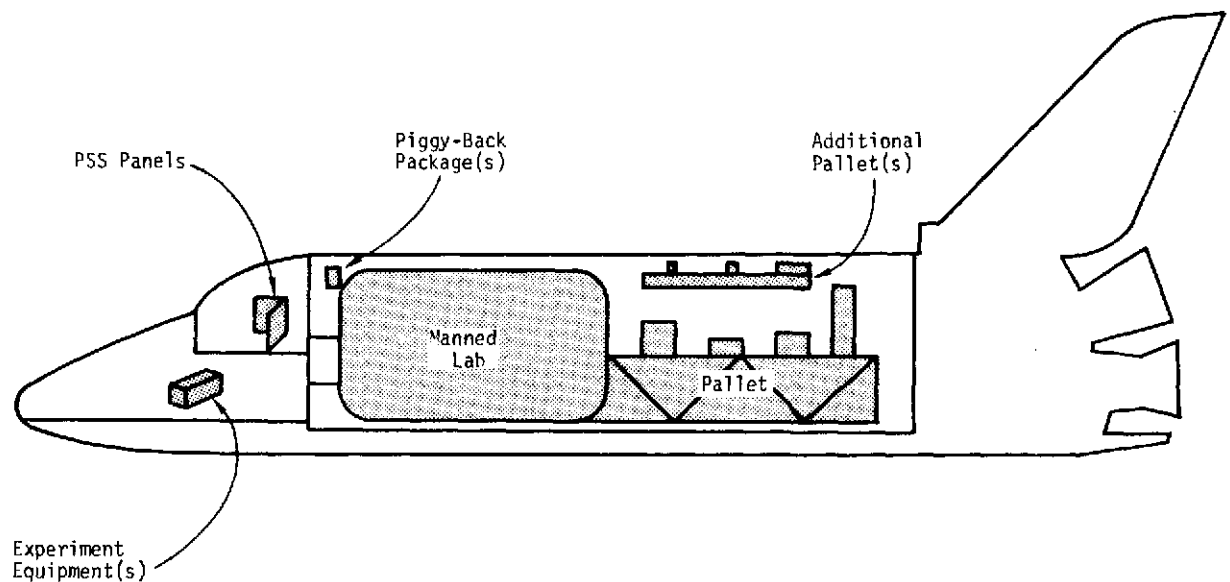


Figure 1-1. Shuttle Sortie Payload Philosophy

Because, in general, sortie payloads are pre-phase A in development, a generalized sortie payload was conceived against which a preliminary hazard analysis could be scoped. This generalized payload model contains the subsystems, instruments, and considerations known to be included in representative sortie payloads and the model is defined in Section 5.

The basic guidelines employed in the study are summarized in Table 1-2.

Table 1-2. Study Guidelines

- This study addresses the post R&D, operational shuttle era assuming a mature, fixed-design, "shuttle airlines" flight operations capability oriented to low-complexity, low-cost operations.
- Design and test considerations include only those imposed by the space shuttle for mission purposes and are confined within the limits from terminal countdown through a normal landing.
- Whether payload equipment is from the civilian sector or GFE should not alter the applicability of the shuttle imposed mandatory criteria. The payload should be given maximum possible latitude.
- Extravehicular activity (EVA) requirements are not excluded from a sortie payload. However, shuttle EVA equipment are excluded from assignment to the payload.
- Study definitions:
 - Criteria are general rules by which the acceptability of shuttle payloads may be determined.
 - Specifications are the translations of criteria into explicit, usually quantitative, statements suitable for detailed design and test purposes. A criterion may translate into several specifications.
 - Requirements may be criteria or specifications which have been imposed by appropriate administrative authority.
 - Crew Safety involves those payload design features that must be satisfied so that any credible hazard (i.e., believable as proven by experience or analytical techniques) is eliminated or its expectance reduced to acceptable limits of risk.
 - Hazards are events or conditions that could cause death or serious injury to one or more of the orbiter personnel through either direct means or indirectly via propagation of vehicle hardware damage (other non-crew-hazard hardware safety considerations are treated as systems compatibility).

Table 1-2. Study Guidelines (Concluded)

- Mandatory crew safety design criteria and verification levels are defined, levied and controlled by shuttle management and are obligatory to all sortie payload elements.
- Discretionary design criteria make up all other criteria. Implementation and verification of these criteria are subject to payload project management prerogatives.

2. PRECEDENT PRACTICES RESEARCH

The "precedent practices" research was the first major task of the study. The objective was to examine past safety practices in order to provide a basis upon which to recommend those practices and safety criteria appropriate for application to Shuttle sortie payloads. Specific candidate safety criteria were accumulated during the course of the historical research.

2.1 APPROACH

The basic approach to the research phase of the study consisted of outlining a research plan containing queries designed to derive needed information, and criteria for selection of the programs to be studied. Implementation consisted of selecting the programs, gathering and analyzing the data from these programs, and iterating appropriate conclusions and recommendations for use in the shuttle era.

2.1.1 Required Information

The first of two parallel efforts defined the information that would be needed to establish the criteria which should be recommended for the shuttle era. The information needed to establish applications to future programs is represented by the seven data search points summarized below in Table 2-1.

Table 2-1. Research Queries Applied to Each Program

- Determine what criteria were used to write payload design specifications that were placed upon experimenters to assure safety. If not available, obtain payload specifications.
- Determine what payload verification criteria or specifications were used to assure man/vehicle safety from harmful payload effects.
- Determine which of these design and verification criteria or specifications were relaxed or revised from their original requirement, and why.
- When criteria were specified, determine the method of application and the philosophy of the criteria.
- Determine which criteria or specifications resulted in high production or verification costs with respect to overall costs.
- Indicate how successful the payload was and if any failures caused safety problems.
- Indicate extent to which off-the-shelf or standard components were used in the payload, and whether failure of these components affected non-vehicle safety.

2.1.2 Programs To Be Researched

In selecting the programs from which this information was desired, attempts were made to choose programs having the most identity with the space shuttle sortie payload situation. The driving considerations were these:

- The program should be analogous to the space shuttle situation, especially where a payload was adapted to its carrier vehicle.
- Most recent programs were studied so that up-to-date technology would be considered.
- Unmanned space programs were studied because of the sortie payload remote (unmanned) characteristics.
- Aircraft research programs were studied because of their operational nature and similarity to the shuttle.

Specific attempts were made to use programs from manned and unmanned spaceflight as well as research aircraft programs such as the Earth Resources Aircraft Program (ERAP).

Manned spaceflight programs were desired because of the direct man-rating aspects; unmanned programs because most frequently the payload is adapted to the carrier vehicle (booster), as will occur with payloads adapting to the shuttle. Aircraft programs are desirable because they are the only programs where principal investigators fly onboard and operate the equipment in flight, as may occur on the Shuttle Program.

Based on these driving considerations, the following programs were selected for study:

● Apollo Scientific Instrument Module Bay	● USAF Satellite Safety Criteria
● Apollo Lunar Surface Experiment Package	● USAF Manned Orbiting Laboratory
● Skylab Experiments	● Pioneer F&G
● CV-990 Aircraft Research Program	● P&F Subsatellite
● Earth Resources Aircraft Program	● Model 35
	● High Energy Astronomic Observatory

2.1.3 Data Search

Information was obtained on the programs by two basic methods: (1) NASA and contractor personnel who were associated with these programs were interviewed, enabling the study team to obtain information pertaining to the early development stages of these programs where pertinent, detailed historical documentation was not available, and (2) current documentation was analyzed to obtain the required information.

While analyzing documentation per the query statements in Table 2-1, safety criteria were extracted and accumulated for later use where they occurred.

2.2 CONCLUSIONS

The conclusions reached as a result of the historical research are listed in Table 2-2.

2.3 RECOMMENDATIONS

Based on conclusions from research and analysis of the past practices, recommendations were made to, and accepted by, the NASA management team at the formal mid-term review. These recommendations affected safety criteria selection and categorization for use in the shuttle era. The recommendations are presented in Table 2-3.

Table 2-2. Conclusions from Precedent Practices Research

CONCLUSIONS	PROGRAM TYPE		
	MANNED SPACE	UNMANNED SPACE	AIRBORNE SCIENCE
1. JSC has evolved a comprehensive set of safety requirements and guidelines. These requirements and guidelines form a base from which mandatory space shuttle imposed requirements can be drawn.	X		
2. Safety requirements and guidelines are not presently accumulated into a central source document.	X		
3. Past and current programs have been primarily research and development in nature, and have levied extensive safety requirements on hardware.	X	X	
4. Operational airborne experiment carriers levy significantly fewer safety requirements on instrument hardware as compared to manned spaceflight systems.			X
5. Present safety requirements and guidelines reflect a conservative research and development approach. If this approach and these requirements are utilized in the shuttle era, the space shuttle operational capability will be severely technical and cost constrained.	X	X	
6. Historically, safety in experiments was achieved by the safety discipline adding necessary safety requirements to a spec. All safety requirements were then treated as subsystem design requirements. Safety involvement was then required only when non-compliance occurred.	X		
7. Current safety efforts have been oriented toward more involvement. In addition to safety requirements, a hazard analysis and periodic reporting are required.	X		
8. Research to date demonstrates that only government equipment or instruments have been utilized on manned space flight.	X		

Table 2-2. Conclusions from Precedent Practices Research (Concluded)

CONCLUSIONS	PROGRAM TYPE		
	MANNED SPACE	UNMANNED SPACE	AIRBORNE SCIENCE
9. Flight safety requirements are crew oriented in vehicles. Ground safety requirements are ground personnel oriented.	X	X	X
10. On programs to date, safety design requirements have been mandatory, but requirements which could not be met were frequently waived. Efforts to comply with a requirement which can not be met are expensive, as is the processing of a waiver. Money spent in both of these areas can not be recovered.	X	X	
11. Compliance with design requirements is verified primarily by testing, which is the method of verification most used by NASA.	X	X	X
12. Testing has been a major portion of program schedule and program cost.	X	X	X
13. Testing to verify a safety requirement is seldom identified directly because most safety requirements are levied as design requirements. Compliance with the requirement is then verified as a part of subsystem testing.	X		
14. Overall cost can frequently be lowered by designing to a greater load factor than can be imposed, then eliminating testing requirements. For example, on one aircraft program, instrument mounts are designed for up to 9g loading with only analytical verification required, where the maximum stress which can be imposed by the aircraft is 3.5g.			X

Table 2-3. Recommendations from Precedent Practices Research

RECOMMENDATIONS	CONCLUSIONS REFERENCES
1. A payload preliminary hazards analysis should be completed to insure the accumulated safety requirements base will contain the mandatory set of requirements.	1, 2
2. The safety requirements and guidelines base, verified by the hazard analysis, form the candidate criteria base which will be examined in this study.	1, 2
3. Use should be made of experience gained in manned space programs, but a transfer from an R&D to a scheduled operational approach should be effected.	3, 4, 5
4. The present mandatory set of safety requirements should be reduced by: <ul style="list-style-type: none"> • Use of aircraft-oriented requirements where the space shuttle is most similar to an aircraft. • Use of spacecraft-oriented requirements where the space shuttle is most similar to a spacecraft. 	4, 5, 9, 10
5. Mandatory requirements for crew safety should be applied equally to a NASA procured instrument or any independent payload developer's instrument.	4, 6, 7, 8, 9
6. The mandatory set of requirements should be imposed on payload instruments. A mandatory set of safety requirements should not include functional operation success requirements.	3, 5, 9, 10
7. Experience gained to date in space flight should be used to accomplish verification by the least expensive method which will provide sufficient assurance of compliance.	11, 12, 13, 14
8. The mandatory safety testing requirements should not include any unnecessary testing of instrument functional capability.	11, 12, 13, 14

REPRODUCIBILITY OF THE
ORIGINAL PAGE IS POOR

3. CATEGORIZATION PROCESSES DETERMINATION

The objective of this task in the Crew Safety Criteria Study was to use an analytical approach in the formulation of a methodology and associated rationale for distinguishing between mandatory and discretionary design and verification criteria for shuttle sortie payloads.

3.1 APPROACH

A series of analytical steps forming a logic tree was developed as the most objective method to determine categorization now and in the future. Several assumptions and guidelines form the basis of the sequential steps of each of the two processes; the first process to determine the category of a design criterion, and the second process to determine the level of verification required to show compliance with a particular design criterion. The basic definitions and guidelines used in addition to the study guidelines iterated in Section 1 are these:

- The set of mandatory criteria which must be imposed by the shuttle for crew safety is not a function of the state of development of the instrument. An instrument being designed should be required to meet exactly the same crew safety criteria as any other off-the-shelf or existing inventory instrument.
- The definition of safety will be "hazard to the crew" and includes vehicle hardware damage only where crew safety is involved.
- An assumption was made that all mandatory criteria require some form of verification, and discretionary criteria verification would not be mandatory.
- The process will first examine candidate criteria to determine that they are sortie payload crew safety criteria. Then, to determine that each criterion is either mandatory or discretionary, it is necessary to examine the severity of consequence of not applying the criterion.

Both the design and the verification categorization processes, because of their general nature, can be used to categorize safety criteria now, and as further definition of payloads occur within the shuttle program, the

processes can be modified to be more specific in nature. This modified process, together with guidelines representing the specific situation under study, allows NASA to use these categorization processes as a means of determining whether a particular criterion is mandatory, together with substantiating rationale, to protect the crew from injury by malfunction of a payload.

3.2 DESIGN PROCESS

The objective of the design categorization process is to determine whether each candidate criterion is mandatory or discretionary with respect to crew safety. This was done by determining that the criterion under consideration was applicable to a sortie payload and would apply to crew safety. Subsequently, the result of not imposing the criteria is analyzed. A block-by-block discussion and analysis of the main vein of the Crew Safety Design Categorization process, which is presented in Figure 3-1, follows.

Block 1. Is the criterion applicable to the payload class under consideration?

The determination here is to determine if the criterion can be applied to a sortie payload. More detailed screening of each criterion involves determining whether that criterion applies to a possible subsystem of a sortie payload or to a subsystem which is precluded as part of a sortie payload, such as, propulsive system, or satellite, or tug ejection mechanism. Those criteria found not to apply to a sortie payload are held for separate delivery to NASA.

Block 3. Does the criterion address a hazard that could endanger the crew?

The determination is made here as to whether a hazard is being controlled which applies ultimately to crew safety or compatibility where hardware is being protected from other hardware. Those criteria found not to apply to a crew hazard were referred to the Systems Compatibility Criteria Study for analysis, and the categorization process continues for those which apply to crew hazard.

REPRODUCIBILITY OF THE
ORIGINAL PAGE IS POOR

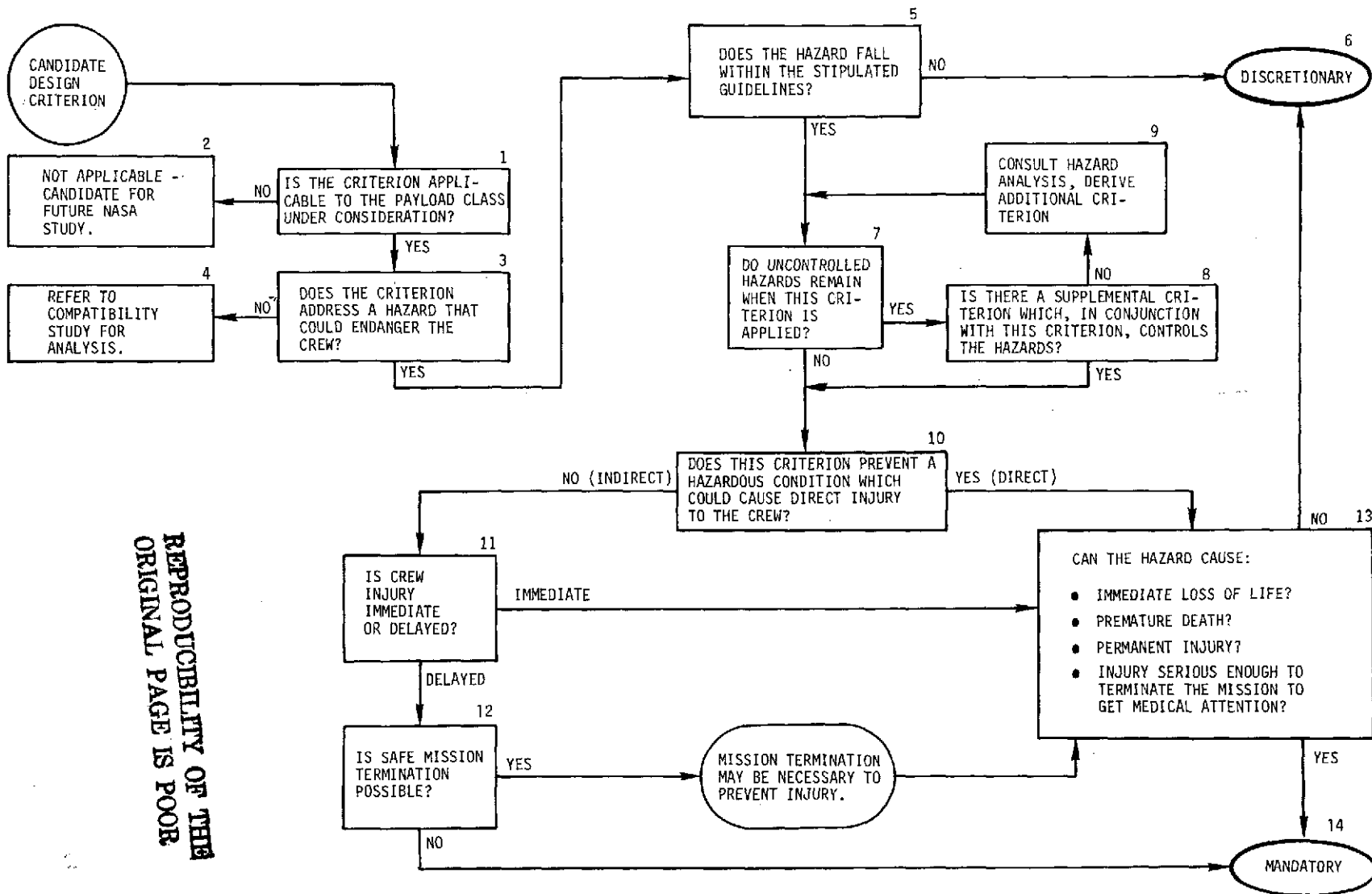


Figure 3-1. Crew Safety Design Categorization Process

Block 5. Does the hazard fall within the stipulated guidelines?

The guidelines under consideration influence the decision at this point. For Block 5, the guidelines introduced in Table 1-2 are used. In future uses by NASA, other stipulations may be used such as more liberal definitions for the credibility of hazards and/or matters of NASA policy.

Block 7. Do uncontrolled hazards remain when this criterion is applied?

The intent of this question is to determine if applying the criterion under consideration protects the crew from this hazard, or is the hazard only partly controlled and additional criteria required to control the hazard. Note that this question does not refer to other, similar hazards which must be controlled by other criteria. An example of the use of this block can be found in F-8 in Table 6-9, which requires shutting off air circulation in the event of a fire. Two uncontrolled hazards remain: no breathable atmosphere (required by E/I-18 in Table 6-4) and fire suppression (required by F-7 in Table 6-9). Thus, the three criteria together completely control the hazard.

Block 10. Does this criterion prevent a hazardous condition which could cause direct injury to the crew?

At this point in the process, it was found worthwhile to separate the situations where a direct payload to crew interface exists (and injury can be direct via this interface) from indirect injury (where damage to the shuttle could propagate to the crew member). This is a major branch in the design criteria categorization methodology.

This branch was necessary because of distinction between the manner of crew injury. In the direct case, the crew/payload interface is considered. In the indirect case, hardware damage is considered, and payload to vehicle interfaces are addressed using the shuttle model to determine the extent of possible vehicle damage which could result in crew injury.

Block 13. What is the extent of the possible injury?

Upon entering Block 13, we have determined that the hazard is appropriate for consideration and that injury to the crew member is possible.

In Block 13, the determination is made of the extent of injury induced by the payload hazard if the criterion is not imposed. Four questions are asked in what might be called decreasing order of severity. These four questions encompass all crew injury which would be beyond the onboard medical capabilities and would require mission termination for medical aid.

- Is there immediate loss of life? Immediate loss of life is defined as a situation where death would occur before the mission could be aborted.
- Is the injury terminal? This question refers to injury of a sort (such as a radiation overdose) which would shorten the life of the crew member, but has no immediate physical impairment as far as the mission is concerned.
- Is the injury permanent? Permanent injury is defined as an injury from which the crew member could not recover, such as loss of an eye or a limb.
- Is the injury sufficiently serious to require termination of the mission in order to obtain medical aid? A major injury such as a broken arm, serious bleeding, or some physical problem could, in the judgement of the crew and mission control personnel, require aborting the mission in order to obtain medical aid.

An affirmative answer to any one or more of these four questions is sufficient grounds for the criterion to be considered a mandatory design criterion. A negative answer to all four questions will generate a discretionary criteria decision indicating that there may be only a minor crew injury which has basically no effect on the mission or lasting effect on the crew member(s), and is within the onboard medical capabilities. Assurance that a hazard would, in fact, cause minor damage or injury to the crew can be more easily determined during phase C and D of payload development, and thus has been built into the process here to make the process more usable in the future.

Block 11. Is the injury to the crew member immediate or delayed?

Upon entering this block from Block 10, we have determined that a payload malfunction involving a crew hazard treated by a particular criterion may cause vehicle damage which can propagate to cause indirect crew injury. A distinction is made in Block 11 to determine whether this hazard, which can propagate to the crew, will propagate immediately or can occur after a time delay. The time delay is defined as sufficient for a normal mission termination.

The distinction being made here is basically the same as whether emergency abort procedures will be used, or the crew has time to perform part of a mission timeline and then perform a normal deorbit and entry. The abort mode can involve hazardous operations which are not present in the delayed situation.

Block 12. Is safe mission termination possible?

Upon arrival at Block 12, we have determined that a hazard which can cause indirect, and delayed (there is time for a early mission termination) injury to the crew exists. Since the injury is indirect, vehicle damage must exist. Block 12, therefore, addresses the condition of the shuttle.

Subset questions might be

- Can damage to the shuttle be such that it is aerodynamically unstable?
- Might the payload bay doors be damaged and cannot be closed?

A negative response to the block question indicates payload damage to the vehicle which prevents entry, making the criterion mandatory. An affirmative response, indicating minor vehicle damage, leads to an assumption that delayed injury can occur to the crew as a result of the vehicle damage, thus, making it necessary to terminate the mission early if the injury is significant. The injury situations in Block 13 are again considered.

3.3 VERIFICATION PROCESS DETERMINATION

The objective of verification is to assure compliance with a particular mandatory design criterion. Study of the five basic methods of verification as defined in Apollo Test Requirements (Reference 1) was undertaken to determine under which circumstances each type of verification could be considered sufficient to assure compliance.

As was brought out in conclusions (Table 2-2) from the precedent practices research, experience obtained in spaceflight and spaceflight hardware construction should allow selective easing of verification requirements. Since the first five verification methods listed below are generally less costly than testing of an article, overall programmatic cost savings can be realized for sortie payloads if testing can be de-emphasized.

The verification process presented in Figure 3-2 is designed to determine, for each mandatory design criterion, the minimum method of verification which can be used to show compliance with the design criterion. If verification by a method other than testing is sufficient, then testing of the article to show compliance is discretionary verification to shuttle management.

Block 1. Similarity

Perhaps the most basic method of verification is by similarity. That is, where a space qualified component is being used in an application similar to that for which it was originally designed. It has been found that frequently equipment verified for flight on manned aircraft (such as the ERAP Program) would be sufficiently qualified to allow the component to be considered qualified for spaceflight. An example of this would be vehicle-induced environment.

Block 2. Analysis

Analysis may be used in situations where stress and thermal analyses are performed and, because of uncertainty, safety factors are frequently applied. Under conditions where sufficiently high safety factors are applied, it can be clearly shown by analysis that a hazard has been controlled and, therefore, actual testing is not required.

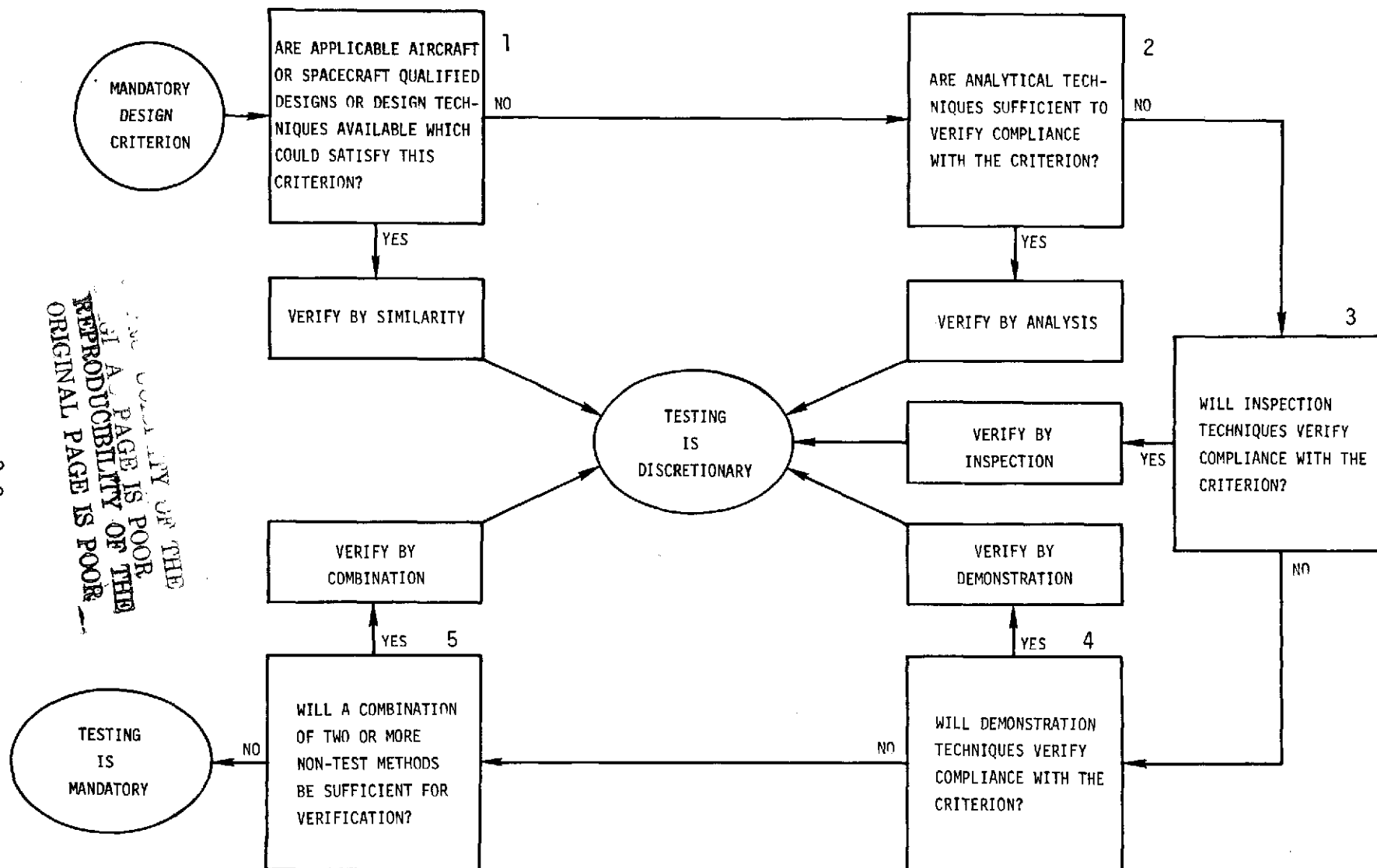


Figure 3-2. Verification Process

Block 3. Inspection

Frequently, verification can be achieved by inspection of a drawing to which the hardware will be built. This type verification is most commonly done at design reviews. A schematic drawing, for example, showing an arming circuit activated by one switch and a firing circuit activated by a second switch would be sufficient verification of the mandatory pyrotechnic design criterion (ED-2) found in Section 6 of this report. Inspection can also include a physical examination of the article, such as inspection of measurements, shape, or the materials of construction.

Block 4. Demonstration

Demonstration is usually restricted to verification of a man/equipment interface. This method of verification can be used to demonstrate that an astronaut can physically perform tasks such as twisting handles or reaching positions on equipment.

Block 5. Combination

Verification by combining two or more of the previously discussed methods may be utilized if one method does not provide minimum acceptable verification.

If none of the four verification methods or any combination of the four can provide sufficient assurance of compliance with a particular design criterion, then verification by testing will be required.

4. CANDIDATE CRITERIA DETERMINATION

Pursuant to the study direction, NASA/JSC agreed to furnish the basic set of safety criteria. These were complemented by requirements accumulated during the past practices research and by a hazard analysis.

Safety Program Directive No. 1 (Reference 2) defines a hazard reduction precedence sequence which is paraphrased below:

- 1) Design for minimum hazards
- 2) Apply appropriate safety devices where design is incapable of eliminating the hazard
- 3) Apply warning devices where some hazard cannot be precluded
- 4) Develop special procedures to counter a hazard
- 5) Identify residual hazards which cannot be eliminated

The candidate design criteria were developed with consideration of this sequence.

This study took the position that all hazards can, in effect, be "designed out" or controlled by the application of a safety or warning device. The criteria address these first three categories of the hazard reduction sequence. Procedural statements were rewritten wherever possible as design criteria rather than procedural statements. The basis for this position is that procedural statements should be developed only when it can be shown that the first three categories (all involving design) cannot control the hazard. This cannot be shown until design efforts have proven fruitless, and current shuttle payload design is in an infancy stage. The procedural statement was rewritten as a design criterion and retained to help insure that no hazards were overlooked. For the same reason, no residual uncontrolled hazard can yet be identified.

4.1 PRIMARY SOURCES

The first conclusion of the Precedent Practices Research Phase of the study states that NASA/JSC does have a comprehensive set of safety requirements and guidelines. The primary source of data for this study phase was the JSC Safety Office who made available (among other documentation) five significant safety studies (References 3 through 7) which had been performed for JSC, NASA Headquarters and MSFC over the period of the last two years. These studies, listed below, supplied a large number of the safety requirements and guidelines and much useful background information about applicabilities and constraints which were used in the Precedent Practices Research Phase.

- Preliminary Hazard Analysis of Space Shuttle Payloads and Payload Interfaces (MSC)
- Safety in Earth Orbit Study (NR)
- Advanced Mission Safety Study (Hqtrs/Aerospace)
- Systems Safety Guidelines for New Space Operations Concepts (MSFC/LMSC)
- Manned Space Flight Nuclear Safety Study (MSFC/GE)

Documentation from all of the programs and collective stand-alone NASA documents such as MSCM 8080 which were reviewed during the Precedent Practices Research Phase of the study were sources of existing requirements. The most significant of these documents are summarized below (References 8 through 13). These six documents, coupled with the referenced safety studies, supplied virtually a complete set of requirements and guidelines.

- Manned Spacecraft Criteria and Standards (MSCM 8080)
- Space Flight Hazards Catalog
- Space Vehicle Design Criteria Manual
- Radiation Protection Guidelines and Constraints for Space-Mission and Vehicle-Design Studies Involving Nuclear Systems
- Standard Satellite System Safety Design Criteria
- System Safety Design Handbook

All of the sources reviewed represent past and current safety practices and supplied existing requirements. These requirements needed to be modulated by the most current shuttle design information. The shuttle model used was supplied by JSC as was Space Shuttle Baseline Accommodations for Payloads (Reference 14).

4.2 APPLICABLE HAZARD AREAS

The following twelve hazard areas stem from the traditional hazard areas listed in the Safety Program Directive No. 1 (Reference 2), as applicable to this study, falling within the study boundaries and guidelines.

- Explosive Devices
- Energy Source Isolation
- Materials Compatibility
- Ionizing Radiation (including Nuclear Device Considerations)
- Fuels and Oxidizers Considerations
- Pressure Vessels
- Electrical Shock
- EVA/IVA
- Contamination (including Toxicity)
- Fire
- Systems Interactions
- Structural

The following hazard categories were not addressed because these categories are either outside the scope of the study (as defined in Section 1) or are not applicable to sortie payload hardware.

- Crashworthiness
- Documentation for sole operation and maintenance
- Training and certification
- Egress, rescue, survival and salvage
- Docking considerations
- Long term storage
- Human factors

4.3 CRITERIA SYNTHESIS

The initial accumulation of candidate safety requirements and guidelines involved extracting each statement found in all documents reviewed, with no regard for redundancy or non-applicability. The statements were then sorted by hazard area and those found to be clearly not applicable to any sortie payload hazard area were eliminated.

Nearly 600 candidate criteria were grouped into the 12 applicable hazard areas and by a process of grouping within each hazard area of similar statements allowed the groupings of similar statements to subsequently be synthesized into one criterion statement. A criterion which is synthesized from a group of requirements and guidelines is more general in nature than any one specific design requirement, and is encompassing of the intent of all of the separate requirements and guidelines from which it is composed.

During the course of this period of criteria management, the first two steps of the design categorization process were completed. Criteria found not applicable to sortie payloads or not applicable to crew safety (pursuant to the study definition) were removed and either filed as not applicable or included in the Compatibility Study for consideration (see Volume III of this report). Likewise, safety criteria were received from the criteria management effort of the Compatibility Study. The resulting criteria which were subsequently taken through the process were thereby reduced to the 132 statements which are included in Section 6 of this report.

Those "duplicate" and "not applicable" criteria statements which were removed from further consideration have been retained in separate files and will be delivered to NASA/JSC under separate cover from this report. These criteria represent a comprehensive compilation which will be useful to JSC in other safety work.

5. HAZARD ANALYSIS

The main purpose of the hazard analysis was to generate a capability to cross-check the crew safety design criteria population to insure that all known hazards which could occur on a sortie payload were treated by the criteria. The hazard analysis was performed as a separate effort to the accumulation of candidate criteria, with no interchange. In this manner, objectivity of the hazard analysis is insured.

5.1 ASSUMPTIONS AND LIMITATIONS

The scope of this hazard analysis was broad, thereby necessarily yielding an analysis general in nature. Even though general, the analysis served the useful purpose of defining the scope of the types of hazards that might be found aboard sortie payloads. As new experiments are defined, it is possible that additional specific hazards will be considered.

The basic guidelines of the study were used as boundaries for the hazard analysis. For example, the time limit boundary basically excludes GSE and ground activities from consideration, and the definition of sortie payload eliminates some subsystems from consideration.

In general, only events or conditions that are inherently dangerous in themselves were considered. If design of device A is influenced so that a hazard cannot occur, then malfunction of other equipment can still not cause that hazard to occur on Device A. Events or conditions were not analyzed if:

- Death or injury could be caused by secondary effects such as a laser radiating energy on a pressure vessel causing it to explode, thereby destroying the orbiter. Pressure vessel design criteria should preclude the explosion, by relief techniques, thermal control, etc.
- Death or injury could be caused by out-of-sequence operations, false signals, or failure of system hardware when specific definition of system hardware design is required to determine the effect of the failure.

The twelve applicable hazard areas for this study were used as guidelines, but pursuant to the nature of any hazard analysis, these guidelines were not limiting or binding.

5.2 GENERALIZED SORTIE PAYLOAD

At present, a complete sortie payload does not exist upon which a hazard analysis could be performed. Additionally, analysis of any given sortie payload would not insure a complete analysis, as no one payload will have every conceivable subsystem or material which the analysis must treat.

The basis for this hazard analysis was, therefore, a generalized sortie payload concept generated to represent all hardware subsystems which can occur as part of a sortie payload, and to list considerations or types of conditions which can occur on the sortie payload (such as an experiment containing microbes).

The generalized sortie payload subsystems and considerations are presented in Table 5-1.

5.3 ANALYSIS

The analysis followed the outline of the Generalized Sortie Payload, and therefore, Table 5-1 can be used as an index to the overall hazard analysis output.

The first step in the performance of the hazard analysis was to gather information relating to shuttle sortie payloads, the materials for construction, and known hazards involved in instruments and materials which compose these payloads. Data were gathered from applicable documentation (References 4, 13, 14, and 15).

The next step of the hazard analysis was to identify, from among the materials, subsystems, and particular equipment, identifiable mechanisms for energy release. Associated with each of these energy release mechanisms are one or more hazards, which are identified and listed as a subset of the release mechanism classification. The entire output of the analysis is presented in Table 5-2.

In the later comparison between the hazards identified and the categorized criteria, five hazards were found to exist for which there were no criteria. Applicable criteria were generated and categorized.

Table 5-1. Generalized Sortie Payload Subsystems and Considerations

<p><u>1.0 MATERIAL</u></p> <p>1.1 Metal</p> <p>1.2 Plastic</p> <p>1.3 Composite Material</p>	<p><u>4.0 THERMAL</u></p> <p>4.1 Conduction</p> <p>4.2 Liquid Loop/ Cold Plate</p> <p>4.3 Heaters</p> <p>4.4 Insulation</p> <p>4.5 Radiation</p>	<p><u>7.0 INSTRUMENTS</u></p> <p>7.1 Data Circuitry</p> <p>7.2 Transducers</p> <p>7.3 Electrical Instruments</p>	<p><u>11.0 ELECTRICAL/ELECTRONIC</u></p> <p>11.1 Power Circuitry</p> <p>11.2 Batteries</p> <p>11.3 Power Supplies (AC & DC)</p> <p>11.4 RF Transmitters</p>
<p><u>2.0 MECHANICAL</u></p> <p>2.1 Hatch</p> <p>2.2 Structures</p> <p>2.3 Cryogenic Cooler</p> <p>2.4 Extendable Booms</p> <p>2.5 Antenna</p> <p>2.6 Gyros</p> <p>2.7 Shields</p> <p>2.8 Hydraulics</p>	<p><u>5.0 PNEUMATICS</u></p> <p>5.1 Pressure Vessels</p> <p>5.2 Extending Mechanisms</p> <p>5.3 Valves & Lines</p> <p>5.4 Compressor</p>	<p><u>8.0 AGENTS</u></p> <p>8.1 Reagents</p> <p>8.2 Pathogens</p> <p>8.3 Fuels & Oxidizers</p> <p>8.4 Fluids & Gases</p> <p>8.5 Corrosive Fluids</p>	<p><u>12.0 CREW INVOLVEMENT</u></p> <p>12.1 EVA/IVA</p> <p>12.2 Control Display Interface</p> <p>12.3 Direct Operation</p>
<p><u>3.0 CONTROLS & DISPLAYS</u></p> <p>3.1 Control Stimuli</p> <p>3.2 Display Responses</p> <p>3.3 Computer Operations</p>	<p><u>6.0 ENERGY SOURCES</u> (Also Generating Equipment Considered)</p> <p>6.1 X-Ray</p> <p>6.2 Magnetic Flux (EMI)</p> <p>6.3 Radio Frequency (RF)</p> <p>6.4 Payload Generated Nuclear Particles</p> <p>6.5 Laser</p>	<p><u>9.0 POINTING/AIMING</u></p> <p>9.1 Gimballed Platforms</p>	<p><u>13.0 ENVIRONMENT</u></p> <p>13.1 Pressure</p> <p>13.2 Vibration</p> <p>13.3 Acceleration</p> <p>13.4 Thermal</p> <p>13.5 Humidity</p> <p>13.6 Acoustical</p> <p>13.7 Gravity</p> <p>13.8 Natural Radiation</p> <p>13.9 Contamination</p> <p>13.10 Meteoroid</p>
		<p><u>10.0 PYROTECHNICS</u></p> <p>10.1 Pyrotechnics</p>	

Table 5-2. Preliminary Sortie Payload Hazard Analysis

CATEGORY	SUBSYSTEM DESCRIPTION	HAZARD TO CREW
1.0 <u>MATERIAL</u>		
1.1 Metal	Magnesium Aluminum Beryllium Steel Copper Lithium Fluoride Mercury Potassium Binary Hafnium Compound Potassium Sodium Niobate Gallium Arsenite Alumina	<ul style="list-style-type: none"> • Toxic metal • Fragile metal, unexpected structural failure • Material at high temperature, metal ignition • Flammable metal • Radioactive
1.2 Plastic	Teflon Fiberglass Urethane	<ul style="list-style-type: none"> • Toxic plastic • Fragile plastic • Combustible plastic
1.3 Composite Material	Wood Ceramic Carbon Filament Asbestos	<ul style="list-style-type: none"> • Combustible material • Fragile material • Toxic material
2.0 <u>MECHANICAL</u>		
2.1 Hatch	Hatch	<ul style="list-style-type: none"> • Failure of hatch to function • Sharp edges on hatch • Hatch opens inadvertently • Kinetic energy of hatch when being opened • Crack occurs in hatch and causes decompression • Hatch too small in diameter limiting personnel flow during regular and emergency egress • Failure of expandable hatchway
2.2 Structures	Payload Structure	<ul style="list-style-type: none"> • Structure fails due to fatigue or stress, equipment becomes a projectile • Sharp edges • Caught in structure (EVA activities) • Prestressed members (stored energy) • Bending of structure (whipping action) • Interference with deploying structure
2.3 Cryogenic Cooler	Cryogenic Cooler	<ul style="list-style-type: none"> • Cryogenic fluid leakage (suffocation) • Cryogenic fluid boil off (venting) not occurring properly • Tank burst • Material exposed to cryogenic fluid (material may burn with LOX)

REPRODUCIBILITY OF THE
ORIGINAL PAGE IS POOR

Table 5-2. Preliminary Sortie Payload Hazard Analysis (Continued)

CATEGORY	SUBSYSTEM DESCRIPTION	HAZARD TO CREW
2.0 MECHANICAL (Continued)		
2.4 Extendable Booms	Extendable Booms for Ion Collector Target	<ul style="list-style-type: none"> • Stored mechanical energy • Sharp edges • Rate of movement (kinetic energy) • Bending of boom (whipping action) • Stowing of boom
	Extendable Antenna Telescopic Boom	<ul style="list-style-type: none"> • Inadvertent release • Physical interference with critical system
2.5 Antenna	Extendable Antenna	<u>EVA Activities</u> <ul style="list-style-type: none"> • Sharp edges • Radiating energy
	"Sunflower" Antenna	<u>EVA Activities</u> <ul style="list-style-type: none"> • Bending of structure • Stored energy • Deployment • Inadvertent release • Rate of movement (kinetic energy) • Physical interference with critical system
2.6 Gyros	Control Moment Gyros	<ul style="list-style-type: none"> • Rotating parts (kinetic energy) • Electrical shock • Damping fluids leakage (if toxic or flammable fluid used) • Implosion (vacuum container)
2.7 Shields	Radiation Shields Mechanical Shields Heat Shields Meteorite Absorbing Shields	<ul style="list-style-type: none"> • Radiation • Sharp edges • Asbestos shields • Failure of shield
2.8 Hydraulics	Hydraulic System	<ul style="list-style-type: none"> • Failure of components (bursting) • Moving and rotating parts (kinetic energy) • Ignition of flammable hydraulic fluid
3.0 CONTROLS & DISPLAYS		
3.1 Control Stimuli	Computer Output Control Circuit Manual Command	<ul style="list-style-type: none"> • Electrical shock • Toxic material such as use of selenium rectifier
3.2 Display Response	Alarms Lights	<ul style="list-style-type: none"> • Display malfunction
	Cathode Ray Tube	<ul style="list-style-type: none"> • X-Ray production
3.3 Computer Operations	Computer Process	<ul style="list-style-type: none"> • Shock hazard • Failure of support, equipment becomes a projectile

Table 5-2. Preliminary Sortie Payload Hazard Analysis (Continued)

CATEGORY	SUBSYSTEM DESCRIPTION	HAZARD TO CREW
4.0 <u>THERMAL</u>		
4.1 Conduction	Resistance Furnace	<ul style="list-style-type: none"> Resistance heated furnace (1600°C achievable)
	Oxygen Chamber Furnace	<ul style="list-style-type: none"> Oxygen chamber furnace (3200°C achievable) Failure of conducting element, hot metal spewage
	Thermal Electric Chiller	<ul style="list-style-type: none"> Metals used are toxic
4.2 Liquid Loop/ Cold Plate	Thermal Control Subsystem	<ul style="list-style-type: none"> Line rupture Flammable fluids ignition Toxic fluids Touch hazard, low temperature
4.3 Heaters	Heater Systems	<ul style="list-style-type: none"> Electrical shock Touch hazard High temperatures
4.4 Insulation	Firewall Heat Insulator	<ul style="list-style-type: none"> Toxic outgassing from insulator
4.5 Radiation	Quartz Tube Furnace	<ul style="list-style-type: none"> Touch temp (300°C)
	Induction Furnace	<ul style="list-style-type: none"> Touch temp (1600°C - 2500°C) Plasma electron beam unit (heating)
5.0 <u>PNEUMATICS</u>		
5.1 Pressure Vessels	Heater Systems Refrigeration Systems Cryogenic Systems Pressurized Containers Pressurized Instruments	<ul style="list-style-type: none"> Pressure vessel or instrument ruptures, shrapnel may result Pressure leakage possibly causing structural limits in the cargo bay to be exceeded Leakage of flammable fluids and gases may cause explosion or fires Pressurized vessel or instrument with toxic outgassing Permeability of container Leaking or release of toxic fluids and gases
5.2 Extending Mechanisms	Telescopic Boom	<ul style="list-style-type: none"> Sharp edges Rupture of pressurized portion of boom Kinetic energy
	Rotary Motion Boom	<ul style="list-style-type: none"> Hardware interfaces, individual caught between two items moving relative to each other Gas leaks from pressurized portion of the boom, gas may be flammable or explosive, boom may be immobilized
	Bellows Type Boom	<ul style="list-style-type: none"> Toxic gases leaking from pressurized portion of the boom

Table 5-2. Preliminary Sortie Payload Hazard Analysis (Continued)

CATEGORY	SUBSYSTEM DESCRIPTION	HAZARD TO CREW
5.0 <u>PNEUMATICS</u> (Continued)		
5.3 Valves & Lines	Cabin Pressurization Pressure Vessel Hoses	<ul style="list-style-type: none"> ● Rupture of valve ● Leakage (internal and external) ● Line rupture ● Kinetic energy of whipping hoses or line ● Pressure outlet of gas gun
5.4 Compressor	Compressor System	<ul style="list-style-type: none"> ● Compressor rupture ● Fire in compressor caused by ignition of oil vapors ● Leaks ● Escaping gases vented into wrong space
6.0 <u>ENERGY SOURCES</u> (Also Generating Equipment Considered)		
6.1 X-Ray	X-Ray Source Radioactive Material	<ul style="list-style-type: none"> ● X-Ray radiation (voltage over 15KV) ● Shock hazard ● Radioactive material (approx. 5 microcuries)
6.2 Magnetic Flux (EMI)	Induction Heating Unit Induction Positioning Device Super Conductor Magnet	<ul style="list-style-type: none"> ● Loose objects in induction unit ● RF radiation ● Uncontrolled cryogenic release ● Electrical shock ● Sharp edges ● EMI on other system
6.3 Radio Frequency (RF)	Communication System R.F. Oven	<ul style="list-style-type: none"> ● Electromagnetic Field ● Heating effects ● Shock hazard
6.4 Payload Generated	Radioisotope Power Generator Radioisotope Calibrator	<ul style="list-style-type: none"> ● Radioactive source ● High external temperature ● Ionizing radiation ● Resistance load bank (high temperature)
6.5 Laser	Laser Operation	<ul style="list-style-type: none"> ● Noise ● Exploding components ● Brilliant light ● IR & UV radiation ● X-Ray ● Cryogenics ● Concentrated energy ● Gases ● High voltage ● Heat of laser generator ● Laser beam impingement on other equipment ● Beam impingement on personnel or population

Table 5-2. Preliminary Sortie Payload Hazard Analysis (Continued)

CATEGORY	SUBSYSTEM DESCRIPTION	HAZARD TO CREW
7.0 <u>INSTRUMENTS</u>		
7.1 Data Circuitry	Telemetry Instrumentation (Transducer Circuits) Data Processing Circuits	<ul style="list-style-type: none"> • Electrical shock • Toxic materials (selenium rectifiers) • Outgassing materials
7.2 Transducers	Pressure Temperature Vibration Humidity Smoke Fire Combustible Gases Shock Accelerometer Geiger Counter Photometer Strain Gauges Fatigue Gauges	<ul style="list-style-type: none"> • Radiation source in transducer • Hazardous chemicals • Electrical shock
7.3 Electrical Instruments	Electron Microscope Radiometer Altimeter Cameras Dosimeter (Active) Interferometer Lasers Life Sciences Packages Materials Processing Packages Optical Telescopes Photometers Radiometer Scanners Scatterometer Specimens (Exposure) Spectrometers Terrain Sounder X-Ray Telescope	<ul style="list-style-type: none"> • Toxic gas • Electrical shock • X-Ray radiation (voltage over 15KV)
8.0 <u>AGENTS</u>		
8.1 Reagents	Fuel Cell System	<ul style="list-style-type: none"> • Release of barium oxide • Release of potassium
8.2 Pathogens	Microbiological Experiment Operation	<ul style="list-style-type: none"> • Ingestion of pathogens • Skin contamination with pathogens <p><u>Types of Pathogens:</u></p> <ul style="list-style-type: none"> • Arqobacterium • Tumerfaciens • Pathogenic and highly toxic materials used in electrophoretic separation

Table 5-2. Preliminary Sortie Payload Hazard Analysis (Continued)

CATEGORY	SUBSYSTEM DESCRIPTION	HAZARD TO CREW
8.0 <u>AGENTS</u> (Continued)		
8.3 Fuels & Oxidizers	Fuel Cell System	<ul style="list-style-type: none"> • LOX and LH₂ reaction (explosive combination) • LOX leakage (peculiar dangerous properties) • GOX leakage (peculiar dangerous properties) • LH₂ ignition (fire not visible)
8.4 Fluids & Gases	Cryogenic Cooler Fluid (LN2) Work Bay Pressurize Vessels	<ul style="list-style-type: none"> • LN2 leakage not detected (suffocation) • N2-O2 mixture changes • LHe • LNe • Ammonia, Iodide Cyanide • Carbon tetrafluoride, paraffin hydrocarbon • Iodide Cyanide • Nitrogen Oxides • Diborane • Freon • Formaldehyde • Carbides
8.5 Corrosive Fluids	Cooling System Battery	<ul style="list-style-type: none"> • Liquid oxygen • Gaseous oxygen • Liquid hydrogen • Battery electrolyte
9.0 <u>POINTING/AIMING</u>		
9.1 Gimballed Platforms	Telescope Gimbal	<ul style="list-style-type: none"> • Rate of movement (kinetic energy) • Sharp edges and corners • Failure of gimbal stops
10.0 <u>PYROTECHNICS</u>		
10.1 Pyrotechnics	Pyro Operation	<ul style="list-style-type: none"> • Sound level • Outgasses • Explosion
11.0 <u>ELECTRICAL/ELECTRONIC</u>		
11.1 Power Circuitry	Power Hookup Between Interface Equipment	<ul style="list-style-type: none"> • Static electricity • Fires • Insulation outgassing • Explosion of component • Discharge of capacitor • Heat dissipation
11.2 Batteries	Silver Zinc Battery Nickel-Cadmium Battery	<ul style="list-style-type: none"> • Caustic electrolyte • Sparks • Explosion • Electrical shock • Fires • Leakage of GOX and gaseous hydrogen

Table 5-2. Preliminary Sortie Payload Hazard Analysis (Continued)

CATEGORY	SUBSYSTEM DESCRIPTION	HAZARD TO CREW
11.0 <u>ELECTRICAL/ ELECTRONIC</u> (Continued)		
11.3 Power Supplies (AC & DC)	Power Supply Operation	<ul style="list-style-type: none"> • Exposed low voltage or high voltage leads • Sparks • X-Ray from 15KV source • Corona effect • Toxic gas or material in tube • Hardware failure
11.4 RF Transmitters	Operation	<ul style="list-style-type: none"> • Electrical shock hazard • Fire hazard • Sparking • Capacitor explosion • Radiation damage
12.0 <u>CREW INVOLVEMENT</u>		
12.1 EVA/IVA	Crewman	<ul style="list-style-type: none"> • Lack of control of moving mass • Sharp edges, corners, and rough surfaces • See low-gravity hazards (13.7)
12.2 Control and Display Interface	Control Console	<ul style="list-style-type: none"> • See low gravity hazards (13.7) • Sharp edges and projection
12.3 Direct Operation	Payload	<ul style="list-style-type: none"> • Manual mode operation • Fatigue
13.0 <u>ENVIRONMENT</u>		
13.1 Pressure	Pressure Vessel Payload Lab	<ul style="list-style-type: none"> • Pressure loss • Sudden pressure change • Vacuum
13.2 Vibration	Structure	<ul style="list-style-type: none"> • Excessive vibration • Structural failure • Equipment failure
13.3 Acceleration	Structure	<ul style="list-style-type: none"> • Excessive shock • Excessive acceleration • Direction change
13.4 Thermal	Equipment	<ul style="list-style-type: none"> • High temperature • Low temperature • Excessive temperature change
13.5 Humidity	Payload Laboratory	<ul style="list-style-type: none"> • Lack of humidity
13.6 Acoustical	Payload Laboratory	<ul style="list-style-type: none"> • Excessive noise

Table 5-2. Preliminary Sortie Payload Hazard Analysis (Concluded)

CATEGORY	SUBSYSTEM DESCRIPTION	HAZARD TO CREW
13.0 <u>ENVIRONMENT</u> (Continued)		
13.7 Gravity	Equipment	<ul style="list-style-type: none"> • Lack of familiarity of low gravity effects • Inability to control mass • Effect on human anatomy • Tumbling
13.8 Natural Radiation	Thermal Galactic Cosmic Radiation Van Allen Belt - Electron & Proton Ionizing Radiation Solar Flare Proton Burst Gamma Rays Ultra-Violet	<ul style="list-style-type: none"> • Overdose
13.9 Contamination	Equipment	<ul style="list-style-type: none"> • Experiments with contaminants • Microbiologically and bacteriologically contaminating waste material • Oxidizing environment • Lack of cleanliness • Outgassing • Long term inhalation of non-toxic material
13.10 Meteoroids	Meteoroids	<ul style="list-style-type: none"> • Toxic material • Radioactive material • Cabin pressure loss • Structural damage

6. CREW SAFETY DESIGN AND VERIFICATION CRITERIA

The results of the categorization processing of the criteria are a set of minimum, mandatory and discretionary criteria which are presented in this section. A summary presentation of all criteria in each hazard area is given in Table 6-1. A total of 108 mandatory and 24 discretionary criteria are listed in the following tables:

Hazard Area	Table	M	D
• Explosive Devices	6-2	9	1
• Electric Shock	6-3	3	--
• Energy Source Isolation	6-4	15	6
• EVA/IVA	6-5	20	2
• Materials Compatibility	6-6	4	--
• Ionizing Radiation *	6-7	13	4
• Contamination/Toxicity	6-8	9	--
• Fire	6-9	8	1
• Fuels and Oxidizers	6-10	2	--
• Pressure Vessels	6-11	14	8
• Structural	6-12	6	2
• Systems Interaction	6-13	5	--

*Includes nuclear devices

These criteria are the primary result of the Crew Safety Study. These criteria represent the essence of the minimum mandatory criteria required to insure crew safety with the sortie payloads. Those discretionary criteria included represent a partial listing of discretionary design criteria. Per the Study Scope, pure "hardware safety" where there was no crew impact was a subject of the compatibility study. (See Volume III of this report).

6.1 DESIGN CRITERIA

The design criteria presented in the first column of Tables 6-2 through 6-13 are written in a form which includes a statement of the hazard being controlled.

Table 6-1. Crew Safety Design Criteria Summary

EXPLOSIVE DEVICES (10)	ELECTRIC SHOCK (3)	ENERGY SOURCE ISOLATION (21)
<ul style="list-style-type: none"> ● Inadvertent firing 3M, -- ● Misfire 4M, 1D ● Device Size 1M, -- ● Byproduct Containment 1M, -- 	<ul style="list-style-type: none"> ● High Voltages 1M, -- ● Isolation, Grounding 2M, -- 	<ul style="list-style-type: none"> ● Batteries 1M -- ● Short-Circuit Protection 6M, 1D ● Overload Protection 2M, 1D ● Open-Circuit Protection --, 2D ● EMI 1M, 2D ● Arcing 1M, -- ● Redundancy 1M, -- ● Safing Mechanisms 3M, -- ● Thermal Extremes --, 2D ● Contamination --, 1D
EVA/IVA (22)	MATERIALS COMPATIBILITY (4)	IONIZING RADIATION (INCLUDES NUCLEAR DEVICES) (17)
<ul style="list-style-type: none"> ● Thermal Extreme 1M, -- ● Inadvertent Actuation 3M, -- ● Handling 3M, -- ● Leak Detection 1M, -- ● Safing 2M, -- ● Failure Identification 1M, -- ● Restraint/Tethers 2M, 1D ● Lighting 1M, -- ● Isolation Protection 2M, -- ● Containment 2M, 1D ● Emergency Life Support 1M, -- ● Sound Pressure Level 1M, -- 	<ul style="list-style-type: none"> ● Galvanic Corrosion 1M, -- ● Stress 1M, -- ● Incompatible Materials 1M, -- ● Oxidizing or Insulating 1M, -- 	<ul style="list-style-type: none"> ● Containment 1M, -- ● Activation --, 1D ● Cooling 1M, -- ● Coolant Leaks 2M, -- ● Fire 1M, -- ● Radiation 3M, -- ● Monitor/Control 3M, -- ● Jettison/Recovery 1M, 3D ● Decontamination 1M, --

M = MANDATORY

D = DISCRETIONARY

Table 6-1. Crew Safety Design Criteria Summary (Concluded)

CONTAMINATION/TOXICITY (9)	FIRE (9)	FUELS & OXIDIZERS (2)
<ul style="list-style-type: none"> ● Leak/Spill Prevention & Detection 2M, -- ● Gas/Vapor Generation 1M, -- ● Isolation 2M, -- ● Outgassing 1M, -- ● Particulates 1M, -- ● Micro-Biology 2M, -- 	<ul style="list-style-type: none"> ● Source Limiting 1M, -- ● Self Extinguishing 1M, -- ● High Temp. Isolation 1M, 1D ● Open Flame 2M, -- ● Suppression 3M, -- 	<ul style="list-style-type: none"> ● Leak/Vent 1M, -- ● Cleanliness 1M, --
PRESSURE VESSELS (22)	STRUCTURAL (8)	SYSTEMS INTERACTIONS (5)
<ul style="list-style-type: none"> ● Relief Capability 5M, 1D ● Fastening 1M, -- ● Quick Disconnect --, 1D ● Valves 1M, -- ● Pressure Integrity 5M, 5D ● Monitoring 1M, -- ● Dumping 1M, -- ● Overpressure --, 1D 	<ul style="list-style-type: none"> ● Fragmentation 1M, -- ● Manned Volume Walls --, 1D ● Extension/Jettison 1M, 1D ● Securing 2M, -- ● Container Integrity 1M, -- ● Meteoroid Environment 1M, -- 	<ul style="list-style-type: none"> ● Monitoring/Control 5M, --

M = MANDATORY D = DISCRETIONARY

The rationale for the design criteria is basically a rendition of how the criteria moved through the categorization process to become either mandatory or discretionary. Many of the hazards being treated can cause, for example, an injury which will be either immediate or delayed. This has been included, wherever possible, to lend strength to the need for imposing the criteria. This feature will allow some easing of the difficulty of reconsideration of the criteria during later design phases of payloads.

6.2 VERIFICATION CRITERIA

In the Tables 6-2 through 6-12, the verification column presents the lowest cost level of verification considered appropriate to demonstrate compliance with that particular design criterion to shuttle management. The rationale which substantiates the statement is contained within the verification process (see Section 3.3).

6.3 CRITERIA LIMITATIONS

It has been pointed out that these sets of criteria are restricted to apply within the boundaries and guidelines of this study to sortie payloads. Additional clarification to the user is included here.

6.3.1 Critical

The definition of safety, as used in this study, addresses crew safety. Hardware safety is not included except where propagation of a hardware hazard could impact crew safety. As a result, frequently a criteria statement includes the word "...critical...". A critical system or device is one necessary for the crew's safety such as a pyrotechnic which must fire to release a hazardous device, or the environment control/life support system in a manned pressurized payload.

6.3.2 Ionizing Radiation

The criteria included in this section are expected to be applied to radioactive or ionizing sources which, in the judgement of NASA/JSC offices, have significant activity.

6.4 SUBSYSTEMS CROSS REFERENCE

While in many cases safety criteria are best presented by hazard area, safety criteria are most useful to a specification writer or a hardware designer when presented by subsystems. Therefore, Table 6-14 presents a cross reference from the hazard area to hardware subsystems identified by NASA. In Table 6-14, each criterion number is listed under the heading of all subsystems to which it applies.

Table 6-2. Explosive Device (ED) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
ED-1. Pyrotechnic devices must not be susceptible to inadvertent, untimely ignition caused by electrostatic charge buildup; the EMI environment of the shuttle vehicle and launch areas; or transient ground currents, wherever that ignition can cause shuttle damage or crew injury.	Untimely initiation of a pyrotechnic device could cause damage to the shuttle vehicle (such as the payload bay doors) of sufficient severity to endanger the crew. Immediate injury is possible if the device detonates while the vehicle is on the pad or in periods of high acceleration, or if a pyrotechnic within the manned module detonated at an inopportune time. Delayed injury would likely occur if the device detonates while in orbit. The crew injury would occur either during entry, or because entry is not possible. The criterion is therefore mandatory. Shielding, circuit design techniques, and use of already qualified devices are standard practice.	Test
ED-2. A minimum of two discrete and separate events must be required to initiate a pyrotechnic to preclude accidental firing by a crew member.	This is a credible situation, considering the variety of payloads and quick turn-around, and the inexperience of a possible passenger/P.I. The hazard would normally be indirect in nature, where the pyrotechnic damages the vehicle, causing delayed injury due to possible inability to safely terminate the mission. The hazard could also cause direct serious injury or loss of life where a crew member was nearby (EVA or a pyrotechnic within the manned volume). The criterion is mandatory. These events may be accomplished by crew actions, logic circuits, or software.	Inspection
ED-3. Power circuits must be separated from pyrotechnic circuits. A power circuit adjacent to a pyrotechnic circuit can provide an inadvertent ignition source via induction or a short circuit.	Inadvertent or untimely ignition of a pyrotechnic could cause vehicle damage sufficient to prevent re-entry (in the case of payload bay door damage). Immediate injury or loss of life is also possible in the case of cabin damage by a released object. The criterion is therefore mandatory. Separation can be accomplished by shielding within a harness, or by use of a separate wiring harness.	Inspection
ED-4. To preclude misfire, critical explosive trains must meet existing requirements for electrical termination, bonding to the surface to be severed and sealing against vacuum.	This credible crew hazard (misfire) is controlled by this criterion. This hazard can produce indirect injury to the crew by: a) immediate injury because of failing to jettison a hazardous device; b) delayed injury because of inability to safely terminate the mission (such as inability to close the payload bay doors). In either case, the criterion is mandatory.	Inspection
ED-5. If pyrotechnic batteries are used, critical pyrotechnic logic circuits must receive power from a source other than pyrotechnic batteries. The logic circuits power consumption can cause low voltage and misfire.	Inability to fire a critical pyrotechnic device can cause an unsafe condition for the crew. This is a credible crew hazard, which is controlled by this criterion. Indirect, delayed injury as a result of not being able to safely terminate the mission can occur if this criterion is not applied. The criterion is therefore mandatory.	Inspection

PROPERTY OF THE
 AIR FORCE
 PAGE IS POOR
 UNCLASSIFIED

Table 6-2. Explosive Device (ED) Criteria (Continued)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
ED-6. Critical pyrotechnic devices must have redundant charges, initiators, and logic circuits, such that failure of a single circuit does not preclude the essential operation.	A credible hazard of misfire is controlled by this criterion. Indirect injury could occur to the crew if this criterion is not imposed: a) immediate serious injury could occur if a hazardous item could not be jettisoned; b) delayed injury could occur as a result of an inability to jettison a payload, making safe mission termination impossible. In either case, the criterion is mandatory.	Inspection
ED-7. To insure firing of other pyrotechnic devices in parallel, the design of pyrotechnic circuits must prevent constant power drain in the event the device short-circuits upon activation.	A credible misfire hazard is controlled by this criterion, which prevents a short circuit low-voltage situation. Indirect crew injury can occur if this hazard is not controlled by: a) inability to jettison a hazardous item causing immediate injury, b) delayed injury occurring from inability to safely terminate the mission because of inability to jettison an item. In either case, the criterion is mandatory. Standard design includes a fusistor in the power lead to the initiator.	Inspection
ED-8. Explosive charges such as critical guillotine cutters and other charges must be selected to perform the required job with a minimum charge. Devices must be capable of performing the required job under worst case conditions with TBD margin of safety. Sizing requirements are to minimize over-blast, but assure a complete jettison.	A credible crew hazard is controlled by this criterion. Were this hazard to occur, indirect crew injury could occur: a) delayed, by prevention of safe mission termination (an item hanging by a harness loose in the payload bay); and, b) immediate, by failing to remove a hazard (unstable reactor) and the crew being affected by the hazard. In either case, the criterion is mandatory.	Similarity/Test
ED-9. Pyrotechnic exhaust products must be contained or controlled to prevent ignition of peripheral combustibles or contamination of other subsystems, or direct crew injury.	A credible contamination/fire hazard is controlled by this criterion. Indirect crew injury could occur from a fire in the payload bay (or manned volume) immediately, from fire propagation. Direct injury could occur within the manned volume from blast effect. The criterion is mandatory.	Similarity/Test
DISCRETIONARY		
ED-10a. To insure probability of ignition, critical pyrotechnic control devices must be provided with a dedicated power source.	Lack of electrical power to fire a pyrotechnic device at the required time can cause a serious hazard, resulting in at least delayed crew injury. However, the source of the electrical power to fire the pyrotechnic device is in itself the subject of a cost/benefit trade. In the case of a payload, adding a dedicated battery for its associated pyrotechnics, using the redundant shuttle to payload power may be more feasible as well as safer because of a higher reliability on the orbiter than a supplemental battery. The dedicated source, then, does not eliminate a credible hazard. The criterion is discretionary.	

REPRODUCIBILITY OF THE
ORIGINAL PAGE IS POOR

Table 6-2. Explosive Device (ED) Criteria (Concluded)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
DISCRETIONARY		
<p>ED-10b. Pyrotechnic systems must have a floating ground to help in the protection of devices from inadvertent detonation due to vehicle EPS transients, ground currents, and EMI if they have a dedicated power source.</p>	<p>Current mandatory requirements are written to require a pyrotechnic to be unaffected by EPS transients, ground currents and EMI surrounding the pyro. This criteria then is a redundancy measure, and though desirable, the removal of this criteria cannot cause an injurious situation to the crew. However, if ED-10a is applied, then this criterion is mandatory to isolate the shuttle sources from the dedicated sources, and therefore prevent inadvertent firing via "sneak-circuits" resulting from short circuits within the systems. The criterion is discretionary.</p>	

Table 6-3. Electrical Shock (ES) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
<p>ES-1. Payload equipment having high voltage (>100 volts) components must be designed to prevent a crew member from coming into physical contact with the high voltage.</p>	<p>Electrical shock is a credible crew hazard which is controlled by this design criterion. Death or serious injury could result from high voltage shock and would be a direct injury caused by payload equipment, making the criterion mandatory. Protection may be provided by interlocks, bleeder resistor, insulation, closed cases, etc.</p>	Inspection
<p>ES-2. All payload module cases must be electrically bonded to the shuttle structure per shuttle grounding requirements to prevent electrostatic charge buildup and electrical shock hazard.</p>	<p>This criteria controls two credible crew hazards, with no residual hazard. Electrostatic charge creates an electrical shock hazard to the crew, creates the possibility of discharge and thereby provides an ignition source if flammables are present. The electrical discharge and consequent fire hazard is a credible, indirect hazard which can be delayed by preventing safe termination; or, immediate loss of life or serious injury. The electrical shock hazard poses possibility of direct injury to the crew, with the possibility of serious injury existing. The criterion is mandatory.</p>	Inspection
<p>ES-3. Payload modules with self contained electrical power systems must have these power systems electrically isolated from the payload module case to prevent an electrical shock hazard and prevent the case from being a radiator of internally generated EMI.</p>	<p>This criterion helps to control the credible hazards but cannot control the hazards completely. Criterion ES-2 (above) is required to insure control. The shock hazard could cause immediate loss of life or a serious injury directly to the crew member. A payload case radiating EMI can exceed the EMI limit with danger to vehicle and equipment (such as pyros) which could have an indirect injury effect on the crew, either immediately or delayed. The criterion is mandatory.</p>	Inspection/Test

Table 6-4. Energy Source Isolation (ESI) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
ESI-1. Batteries must be thermally isolated from each other and have adequate heat dissipation provisions to prevent battery overheat and explosion.	Two credible hazards are controlled by this criterion. Direct serious injury or death could occur if the battery is in a manned volume. Indirect, delayed inability to safely deorbit can occur if the battery explodes in the payload bay. The criterion is mandatory.	Analysis/Test
ESI-2. A short or open in instrumentation circuitry must not be capable of adversely affecting other systems which in turn adversely affect the crew or vehicle.	This is a credible hazard, controlled by this criterion, which can indirectly cause injury to the crew by preventing safe mission termination. If not properly designed, a short or open can affect the electrical circuitry within a system causing loss of the system. Loss of a system which can interfere with the orbiter can in turn adversely affect the crew (short causes loss of power to boom extension mechanism). The criterion is mandatory.	Test
ESI-3. Electrical wiring must not be in contact with fluid containers. A short from conducting wiring to the line or tank can cause loss of system integrity with resulting release of hazardous fluids, fires and propulsive venting.	This criterion is designed to protect the vehicle and crew from credible hazards, and control these hazards. Any crew injury resulting from the hazards stated would be indirect in nature. A fire or explosion would damage the vehicle, and either prevent a safe termination (delayed) or propagate and cause serious injury or death immediately. Any uncontrolled venting would cause immediate serious injury. The criterion is mandatory.	Inspection
ESI-4. Electrical wiring must not be routed near sharp edges. Chafing of the wiring can cause short circuits, resulting in fire and circuit overload hazard.	This criterion controls a credible hazard. Indirect, immediate crew injury can occur if the short occurs in the open payload bay and fire results. Direct, immediate crew injury can occur if the short occurs in the manned volume where fire can injure the crew. The criterion is mandatory.	Inspection
ESI-5. Adequate provisions must be made for maintaining separation of coolant and electrical components in pump where the fluid loop is critical or the pump is in the manned volume.	In the manned volume, there is a possibility of fire when the pump shorts out causing arcing. This is a credible hazard, with the possibility of fire in the cabin and direct injury or death a possibility. This criterion controls the hazard, and is therefore mandatory.	Demonstration
ESI-6. Electrical circuits which can be cut by guillotine cutters must be protected against short circuits and the resultant circuit overload and fire hazards.	Two hazards are credible, controlled by this criterion, and can cause indirect, immediate crew injury or death. A short to the blade can burn the blade, causing a non-sever hazard, which presents an indirect, delayed hazard to the crew by preventing safe mission termination (something flopping around in the payload bay). The short can also cause a fire hazard by providing an ignition source. The criterion is mandatory in either case. Standard design is to deadface the harness before firing the guillotine.	Inspection

REPRODUCIBILITY OF THE
ORIGINAL PAGE IS POOR

Table 6-4. Energy Source Isolation (ESI) Criteria (Continued)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
ESI-7. Electrical equipment, wiring, and connectors must be positively protected against moisture to preclude short circuits, arcing and resultant fire hazards.	This credible hazard is controlled by this criterion. The possibility of a fire as a result of an arc or short circuit could cause an indirect inability to terminate the mission safely (delayed effect) or immediate loss of life or serious injury, making the criterion mandatory.	Test
ESI-8. Capability must be provided to switch off all electrical loads to a payload from the orbiter to insure control and safing capability should a hazardous situation occur.	A hazard requiring safing is a credible possibility and could cause indirect injury to the crew. No residual electrical hazard could occur if this criterion is applied. If the criterion were not applied, damage could be such that safe mission termination would not be possible. It is equally possible that the hazard could propagate to the point where crew injury or loss of life could occur. The criterion is mandatory to prevent these occurrences.	Inspection
ESI-9. Payload modules utilizing shuttle electrical power must comply with overload protection and grounding requirements of the shuttle. This will protect the shuttle from overload, heat, and fire hazards, and the electrical power system from damage.	These credible hazards are controlled by these requirements. Occurrence of this hazard could cause immediate injury or death to a crew member indirectly as a result of shuttle damage due to a fire, making the criterion mandatory.	Inspection
ESI-10. Payload-generated EMI must be within shuttle requirements, such that the payload does not cause damage to critical orbiter systems.	EMI damage to critical systems can cause loss of critical orbiter capabilities (retro-pyros, communications, G&N, etc.). EMI damage is a credible hazard if outside the specified requirements. Payload damage to orbiter critical functions could cause inability to safely terminate the mission. This is a delayed, indirect hazard to the crew, making the design criterion mandatory. Standard design techniques include grounding, shielding, and filters.	Test
ESI-11. Electrical umbilical disconnects between the orbiter and the payload must be separated from hazardous-fluid disconnects, be qualified as explosion proof or have provisions to remove power during disconnect. This is to preclude electrical arc at disconnect, and to preclude hazardous fluids at all times.	Immediate loss of life or serious injury could occur to a crew member disconnecting a live connector in the presence of any flammable gas. This would be a direct effect to the crewman, and is a credible hazard which is controlled by this mandatory criterion. Standard qualified connectors are available.	Inspection

Table 6-4. Energy Source Isolation (ESI) Criteria (Continued)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
ESI-12. Critical, redundant paths, such as system monitoring or electrical power circuits must not be routed through the same connector. Routing redundant paths through different connectors precludes loss of redundancy from a single point failure. (See MSCM 8080, No. 20.)	Loss of redundant paths via a single point failure is a credible hazard which is controlled by this mandatory criterion. Indirect injury could occur, either serious injury or loss of life, or shuttle damage which could preclude safe mission termination, were this failure to remove all monitoring and an undetected hazard occur. The criterion is mandatory.	Inspection
ESI-13. Electrical valve configurations must be fail-safe in nature and removal or interruption of power must not allow release of fluids, or undesired or uncontrolled venting.	An improperly open valve presents a credible hazard to the crew, which is controlled by this criterion. Dumping or propulsive venting allows for indirect, but immediate crew injury (motion). Dumping or venting a hazardous fluid could cause a fire or explosion, either of which could cause immediate crew injury or death by: a) indirect if exterior to manned volume; or b) direct if inside manned volume. For either situation, the criterion is mandatory.	Inspection
ESI-14. Safing mechanisms must be provided to prevent inadvertent actuation of equipment whose actuation could result in an immediate uncontrolled hazardous situation.	Uncontrolled hazards (such as uncontrolled propulsive venting, inflating objects within the payload bay, etc.) can cause spacecraft motion or damage which will injure the crew. This criterion controls the hazard of inadvertent actuation, which otherwise presents a credible hazard to the crew. There would be no residual hazard. Any crew injury would be indirect in nature, although it could be immediate (uncontrolled venting), or delayed because of structural damage precluding safe mission termination. The criterion is therefore mandatory.	Inspection
ESI-15. Where possible crew injury may result, automatic devices must be provided to shut down or prevent operation of payload equipment under unsafe conditions.	Allowing the experiment equipment to operate under unsafe conditions allows a crew hazard to exist. If the equipment is inside the manned volume, direct crew injury can occur. Credible hazards which will be controlled by this criterion can occur during equipment operation which could affect the crew causing direct injury or loss of life. The criterion is therefore mandatory.	Demonstration
DISCRETIONARY		
ESI-16. To preclude loss of bus voltage with loss of one or more batteries, all payload batteries must be capable of isolation from the bus.	Battery isolation within a payload is in the interest of R/QA. Failure of a battery may shut down a payload, but will not interact with the vehicle, as payload-supplied circuits are isolated from orbiter-supplied circuits. No credible hazard can occur, thus the criterion is discretionary. Standard design includes diode and relays.	

Table 6-4. Energy Source Isolation (ESI) Criteria (Concluded)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
DISCRETIONARY		
ESI-17. Payloads utilizing batteries must insure that battery cell terminal connection areas are isolated from any cell or battery venting to preclude corrosion of battery terminal connections, with possible loss of the battery output capability.	Corrosion of the connecting member could cause loss of battery and loss of payload operability. Since fail safe and isolation from orbiter already is required, there is no manned safety impact. The criterion is discretionary as credible crew safety hazard is not involved.	
ESI-18. Automatically operated devices (heaters) in system components (tanks, batteries, etc.) must be designed so as to fail in the off mode. Devices which fail on are a hazard as no control can be exercised.	Devices which can fail on will cause an overheat and consequently a hazardous condition. Prime result would be loss of the system (fluids vented, battery degraded). The excess current drain on the orbiter could be precluded by turning the system down. Over-pressure vents which are required will prevent vehicle damage/crew injury. This criterion then does not protect a crew member from a credible hazard but is R/OA oriented for the payload system. The criterion is therefore discretionary.	
ESI-19. To preclude undetected high resistance or open circuits, swagged eyelets must not be used to form a solderless connection between conductors.	Swagged eyelets may result in high resistance or open circuits, resulting in low power or loss of power to the payload. Loss of power to a fail-safe condition in the payload does not present a credible hazard to the crew. This criterion is discretionary, dealing with the payload's ability to operate.	
ESI-20. To preclude inability to cycle equipment and return to normal operation, non-replaceable fuses and inaccessible circuit breakers must not be used.	The inability of the crew to cycle a payload circuit breaker or replace a fuse and re-start the experiment may cause loss of the experiment. It does not constitute a credible hazard to the crew, and therefore is discretionary.	
ESI-21. Fluid lines must be designed and/or insulated so as to prohibit freezing or boiling of the fluid under static and normal flow conditions or, should freezing or boiling occur, to prevent permanent system damage.	Lines and containers are sized such that there is adequate safety factor to preclude a loss of system integrity. The worst case occurrence, then, is loss of the payload or subsystem. Since the payload can be shut down (and fail safe) loss of the system involves loss of the payload, but no credible hazard can occur, leaving the criterion discretionary.	

Table 6-5. EVA/IVA (E/I) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
E/I-1. To preclude skin burn or reflex injury, IVA crew members must not be exposed to payload temperature extremes (less than TBD, greater than TBD).	This criterion controls a credible crew hazard. Any injury would be of a direct nature. The injury could be serious enough to terminate the mission. Extreme temperatures can burn the skin causing injury. Extreme temperatures can also cause reflex pull away with arm/elbow injury, damage to equipment to rear of crewmember, inadvertent switch actuation, etc. The criterion is mandatory.	Inspection/ Demonstration
E/I-2. Critical payload controls requiring detachable actuating tools must readily show the control position without the tool in place. Detachable tools must not be used if tool non-availability could compromise crew safety. (See MSCM 8080, Nos. 56 and 65.)	Tool non-availability presents a credible hazard which is controlled by this criterion. No residual hazard of this type would occur. Tool non-availability would cause inability to operate control under urgent conditions. Indicator non-availability causes crew members to not know conditions of equipment, both in normal and emergency conditions. These conditions would allow malfunction before correction could be made with resultant crew injury. Inside the manned volume, serious crew injury could result directly. Outside the manned volume, indirect and delayed inability to terminate could occur, also immediate crew injury or loss of life could occur. The criterion is mandatory.	Inspection
E/I-3. Distinctive identification must be made when otherwise identical switches are located on the same panel and the result of out-of-sequence operating could be serious.	Accidental activation of a critical switch can allow hazardous operations to occur (e.g., out-of-sequence), which are precluded by this criterion. Accidental switch activation which can occur on critical systems poses a definite hazard to the crew. Any injury would be indirect in nature (for the equipment outside the manned volume) and could be either immediate injury or delayed inability to safely deorbit. If the equipment is inside the manned volume, injury can be direct and immediate. Out of sequence operation can also be designed out by use of logic circuits or interlocks. The criterion is mandatory.	Analysis/ Inspection
E/I-4. Critical switch/control configurations must not be susceptible to inadvertent actuation. Any coverguard must be designed so that critical switch/control positions can be determined without moving the coverguard to prevent delayed action. (See MSCM 8080, No. 59.)	Accidental activation of a critical switch can allow hazardous operations to occur (e.g., out-of-sequence), which are precluded by this criterion. Accidental switch activation which can occur on critical systems poses a definite hazard to the crew. A residual hazard (E/I-3) has been identified. Any injury would be indirect in nature (for the equipment outside the manned volume) and could be either immediate injury or delayed inability to safely deorbit. If the equipment is inside the manned volume, injury can be direct and immediate. The criterion is mandatory. Standard switch guards can help preclude inadvertent activation.	Inspection

REPRODUCIBILITY OF THE
ORIGINAL PAGE IS POOR

Table 6-5. EVA/IVA (E/I) Criteria (Continued)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
<u>E/I-5.</u> Caution and warning systems must provide timely warning of equipment safety parameters and status of critical control functions (such as airlock pressures, door positions, overboard vents and payload erection/retraction mechanisms) to allow timely corrective actions, and avoid accidents caused by lack of knowing systems configuration.	Safety critical parameters (manned atmosphere), which may go out of tolerance, require timely caution and warning to allow corrective actions to be taken in time to insure crew safety. This credible hazard is controlled by this criterion. The type injury/damage is a function of the out of tolerance subsystem. An ECLS malfunction can cause direct, immediate crew injury or death. Retraction/erection mechanisms can cause indirect, delayed inability to safely terminate the mission. The criterion is mandatory.	Inspection/ Demonstration
<u>E/I-6.</u> Crew members must not be exposed to sharp points or edges (less than TBD radius of curvature) that could puncture or tear the pressure suit during EVA.	Torn suit leaves a distinct possibility of loss of crew member. This credible hazard is controlled by this criterion. Any injury to the crew member would be direct in nature, and serious injury or loss of life can occur with loss of pressure suit integrity. The criterion is mandatory. Standard design such as rounded corners can eliminate this problem.	Inspection
<u>E/I-7.</u> Handles or grips must be provided for physical transport of payload components requiring transport to preclude loss of control during transport. Such components must be capable of withstanding impact of TBD feet per second with a sharp object (TBD radius of curvature) without releasing the contents.	This criterion is to insure the crew is not injured by loss of control of an object, or by release of its contents, both of which are credible hazards. This criterion is sufficient to control this hazard, which, if it occurred, could cause direct serious injury to the crew member by trapping, crushing, or by the release of contents. The criterion is therefore mandatory.	Inspection/ Demonstration
<u>E/I-8.</u> Manned payload modules must provide means for detecting and purging or dumping a toxic, flammable or oxygen-enriched environment (IVA) when such substances are part of the payload.	Allowing undetected environments which allow a hazard to the crew directly endangers the occupants of the manned module and if undetected can also propagate to the flight check. This credible hazard is controlled by this criterion. Any of these atmospheres caused and undetected by the payload allows the possibility of direct serious injury or death by the atmospheres and resultant chance of fire. The criterion is therefore mandatory.	Inspection/Test
<u>E/I-9.</u> Manually operated shut-off valves in manned payload modules must be located so that downstream line rupture will not prevent access to the valves and control of the undesired venting.	Any line rupture interior to the manned volume allows an undesirable pressure situation in addition to attendant hazards directly attributable to the gas or fluid. Any line rupture external to the manned volume causes strong propulsive vents with attendant motion injury. Either situation is a credible hazard which is controlled by this criterion. Inside the manned volume, direct and immediate injury or death could occur. Exterior to the manned volume, erratic motions could cause indirect immediate injury or damage which later prevents safe deorbit. The criterion is therefore mandatory.	Demonstration

Table 6-5. EVA/IVA (E/I) Criteria (Continued)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
E/I-10. To preclude erroneous or hazardous crew action, the primary failure mode of all critical meters or measurement systems must be such as to give an immediate indication that a failure has occurred.	This criterion requires that the crew be informed to ignore an erroneous out-of-bounds indication (unwarranted action not injurious to crew). The crew must be warned it has lost monitoring capability and may not know of an out-of-bounds, which does allow a hazard to the crew. Acting on bad information presented by instruments can lead to a hazardous situation for the crew. This credible hazard, which can be controlled by this criterion, can, if not controlled, lead to either direct or indirect crew injury. Direct injury if the equipment is within the manned volume or crew member is EVA. Indirect injury if equipment is in payload bay. The criterion is mandatory.	Analysis/ Inspection
E/I-11. All payload fluid/gas disconnects must be uniquely keyed, and individually marked to identify the nature of the substance involved; must be positive locking; and must be designed to prevent venting/leakage during or after disconnect. Inadvertent mixing or venting of incompatible fluids or gases must be precluded.	Connecting to the wrong line can introduce the wrong gas/vent and cause reaction damage and overpressure damage which (in a manned volume) can propagate to the crew. Leakage after/during disconnect can introduce overpressure in the manned volume and hazardous gas introduction into the manned volume. These hazards are credible hazards which will be controlled by this criterion. Any crew injury would be direct in nature. Serious crew injury or death to personnel can occur as a result of the hazards listed above. The criterion is mandatory.	Similarity/ Demonstration
E/I-12. All transportable payload items (such as tools, cameras, film magazines) for EVA usage must always be restrainable to either the vehicle, worksite or the crewman. Loose items can drift into positions where they cannot be retrieved, but can do later damage due to high inertia on entry. Loss of a tool necessary to perform a critical function renders a hazard.	Loss of a tool necessary to insure the safety of the crew with respect to a payload is a real possibility, can result on an EVA if this criterion is not applied. Impact from a flying object is also possible if the tool floated into an inaccessible position. In either case, crew injury may result indirectly, in a delayed manner and therefore this criterion is mandatory.	Inspection/ Demonstration
E/I-13. All payload EVA/IVA worksites must be lighted to those required levels (TBD luminous) necessary to assure non-hazardous operation.	Lack of adequate light at an equipment worksite may cause operator error and equipment damage. The equipment damage can be of a type to propagate and injure the crew. There are situations where incorrect operation could lead to crew injury (operating a release mechanism, incorrect switching, etc.) The hazard is credible, and lighting is a contributor, that, in conjunction with criteria E/I-11 and E/I-3, will prevent injury of both an indirect delayed nature to the crew, and direct, immediate injury to a crew member. The criterion is therefore mandatory.	Demonstration

 REPRODUCIBILITY OF THE
 ORIGINAL PAGE IS POOR

Table 6-5. EVA/IVA (E/I) Criteria (Continued)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
<u>E/I-14.</u> Equipment mounted in the payload bay which requires EVA must be positioned to insure that a fully suited EVA crew member cannot become wedged.	A crew member attempting to unwedge himself could tear his suit. He could also complicate the wedging. If it is a single man EVA (Shuttle groundrule), serious injury or death could occur before rescue could be effected. This criterion controls a credible hazard which, if not controlled, could lead to direct injury or death to the crew member. The criterion is therefore mandatory.	Demonstration
<u>E/I-15.</u> Internal and external areas of passageways between a manned payload module and the orbiter must be free from items whose malfunction could damage or otherwise prevent passageway use by the crew members.	The present docking mechanism and passageway to the manned volume is not redundant. Any loss or damage to this passage affects the crew in the manned payload. This criterion will control the possible occurrence of a credible hazard. Crew injury could occur indirectly by the malfunctioned item failing the tunnel and trapping the manned payload personnel. Serious injury or death could occur immediately. The criterion is therefore mandatory.	Inspection
<u>E/I-16.</u> All crew compartment ventilating fans must be protected by devices to prevent entrance of fan damaging debris during zero-gravity conditions. (See MSCM 8080, No. 73.)	Items floating in zero-g could enter and block or damage needed circulation fans, causing a malfunction hazard to the crew. This criteria addresses a credible hazard which can occur in a manned payload. This criterion will prevent this malfunction hazard which would otherwise cause direct injury to the crew within the manned payload. This direct injury can be serious, and if undetected, could cause death via air stoppage/stagnation. The criterion is therefore mandatory. Normal standard design includes filters, screens, and fan location within the system.	Inspection
<u>E/I-17.</u> Shatterable materials must not be used within a manned volume unless positive protection is provided to prevent fragments from entering the cabin/module environment. Photographic equipment that cannot comply with this requirement must be protected by suitable covers when not in use. Cathode ray tubes, if used, must have safety shields. (See MSCM 8080, No. 41.)	Shatterable materials will leave splinters and sharp edges floating in the manned volume which can cut and puncture. This is a credible hazard which can occur within a manned volume. The hazard involved will be controlled by this criterion. Were a shatter to occur within the manned volume, any crew injury would be directly caused by the fragments. Serious injury could accumulate because of the many fragments within the confined crew area. The criterion is therefore mandatory.	Inspection
<u>E/I-18.</u> Emergency life support must be provided for all personnel in a manned payload module sufficient to allow escape or time to control a fire or toxic spill.	This criterion is to protect the crew from loss of the manned payload environment control/life support system (by shutoff, fire, toxic contaminant) which is a credible hazard. No residual hazard exists if this criterion is applied. If this criterion is not applied, loss of the environment control/life support system of a manned payload can cause indirect, immediate crew serious injury or death. The criterion is mandatory.	Inspection/ Demonstration

Table 6-5. EVA/IVA (E/I) Criteria (Concluded)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
<u>E/I-19.</u> Payloads with a transmission medium (such as air or structure) must not generate sound pressure levels in excess of TBD dB, or crew injury will result.	Excessive sound pressure levels (such as the high discomfort region) cause discomfort and distraction to the crew, increasing the possibility of crew error and a resulting hazard. Beyond the discomfort level is the pain level, and beyond that, physical injury to ear or brain. This credible hazard will be controlled by this criterion. Excessive sound pressure levels for some duration will be a direct source of injury to the crew. The criterion is mandatory.	Demonstration
<u>E/I-20.</u> Payload equipment utilizing mechanical motion which can trap, cut or otherwise injure the crewmember must prevent crew contact with the moving parts.	Equipment such as high speed tape recorders, gears, etc., pose a hazard to the crew. This credible hazard will be controlled by this criterion, preventing direct injury to the crew which would occur with contact. Standard design practice includes shielding, covers or interlocks to prevent contact or stop motion if resistance is incurred. The criterion is mandatory.	Demonstration
DISCRETIONARY		
<u>E/I-21.</u> All payload worksites must have provisions for crewman restraints.	Attempting to perform a job without proper restraint is not possible (pushing in pushes the crew-member away). There is a shuttle ground rule saying crew-member must be tethered. This criterion applies to a sortie payload and a credible hazard exists (hardware), but the hazard does not present a credible hazard to the crew member. This is a crew/payload compatibility problem. The criterion is discretionary.	
<u>E/I-22.</u> Painting or coating materials subject to flaking must not be used in payload equipment that is expected to be exposed to extensive abrasion or contact by crewman (in the manned volume). (See MSCM 8080, No. 43.)	Paint chips and flakes loose in the manned volume can interfere with operations. There is not significant possibility of crew-member injury, such as by flakes being inhaled, etc. Manned spaceflight experience has shown that the possibility of crew injury is not credible. The criterion is discretionary.	

Table 6-6. Materials Compatibility (MC) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
	MANDATORY	
<p><u>MC-1.</u> To preclude metal failure on critical systems (mountings, high pressure, hazardous fluids, etc.), metals of differing potentials must not be combined. (See MSCM 8080, No. 63.)</p>	<p>Galvanic corrosion developing at critical points causes weakened metal and eventual failure. One must consider more than the 30-day mission time on critical systems since corrosion starts at assembly, not at flight time. This criterion controls a credible hazard, and does not leave a residual hazard; a) if in the manned volume, such failure could cause direct injury or death, such as from flying objects or b) if outside the manned volume, the failure could cause delayed inability to safely deorbit due to damage caused by the failure. The criterion is mandatory. Standard design requires appropriate selection, plating, or separating (such as spaces).</p>	Inspection
<p><u>MC-2.</u> Incompatible materials must not be allowed to combine where the result of the combining can cause a hazard to the crew. (Included here are such combinations as flammables with liquid or high pressure oxygen, and mutually reactive materials including hypergolics).</p>	<p>This hazard is a credible hazard, controllable by this criterion with no residual hazard. Inside a manned volume, such a combination can cause direct and immediate serious injury or death to the crew. Exterior to the manned volume, a fire is an indirect, but immediate injury to the crew, possibility of death is very strong. The criterion is mandatory.</p>	Inspection/Test
<p><u>MC-3.</u> Materials which can react with electronic equipment to oxide or form an insulating barrier between contacts (such as sulphur) must not be used in proximity to critical electrical equipment.</p>	<p>Some materials (such as sulphur) can outgas and combine with the copper or other conductor to form an insulation coating, with consequent loss of electrical circuits as well as payload circuits. Loss of a critical electrical circuit could become a real possibility, and is a credible hazard with no residual if this criterion is applied. The damage to the crew is indirect and delayed. Safe termination could be prevented, or, may be necessary to prevent some down-stream-in-time danger to the crew. The criterion is mandatory.</p>	Inspection
<p><u>MC-4.</u> To prevent loss of systems integrity on structural mountings, connectors and sleeves on fluid lines and structures must be of a material resistant to stress corrosion cracks when 1) torqued to required levels and 2) exposed to expected environment. (See MSCM 8080, Nos. 14 and 113.)</p>	<p>Stress corrosion and metal fatigue failure can cause loss of structure on the pressure system. The hazard which can occur is a credible hazard with no residual hazard if this criterion is applied: a) If the pressure system were ECLS or in the manned volume, direct and immediate crew injury could occur; b) if the pressure system or structure is outside the manned volume, indirect and delayed injury to the crew is possible, with safe mission termination not possible. In either case, the criterion is mandatory.</p>	Similarity/ Inspection/Test

Table 6-7. Ionizing Radiation (IR) Criteria*

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
<p><u>IR-1.</u> Fragmentation, blast over pressure and fireball protection adequate to assure containment of all radioactive material must be provided by the isotope-source payload supplier to preclude release of radioactive material should a shuttle accident occur.</p>	<p>Any radioactive leak endangers the crew with overdose and also contaminates the vehicle. This criterion is to protect the crew against a credible hazard. This criterion would allow direct injury, most likely, premature death resulting from overdose. The criterion is mandatory.</p>	Test
<p><u>IR-2.</u> Nuclear device payload suppliers must assure that critical nuclear subsystems are maintained at proper temperatures to remain stable.</p>	<p>Some payloads may have sodium-potassium loops which may freeze and rupture at cold temperatures. Some Brayton-type systems require constant cooling. In either case, the criterion is to eliminate a credible hazard to the crew. No residual hazard exists if this criteria is applied. Since over temperatures may result in release of radioactive material resulting in direct injury or premature death to the crew, this criterion is mandatory.</p>	Inspection
<p><u>IR-3.</u> Reactor payloads must preclude any leak of sodium-potassium coolant. Exposure of the sodium to oxygen will result in a liquid metal fire.</p>	<p>This criterion is designed to eliminate a credible hazard. No residual hazard will exist. A liquid metal fire could propagate to the crew and therefore cause indirect, immediate crew injury. The criterion is therefore mandatory. Standard design includes double containment and inert gas blankets while in the atmosphere.</p>	Pressure Test
<p><u>IR-4.</u> The design of payload reactor coolant loops that use sodium-potassium as a primary coolant must not require breaking or opening during orbital operations. The sodium-potassium may be at very high temperatures and the EVA suit is incompatible with the liquid metal.</p>	<p>This criterion is designed to prevent the occurrence of a credible hazard to the crew. No residual hazard is allowed, and serious crew injury or death could occur directly from exposure to sodium-potassium if the criterion is not applied; therefore, the criterion is mandatory.</p>	Inspection
<p><u>IR-5.</u> A liquid metal fire suppression system must be provided by the nuclear reactor payload for use at any time the orbiter is in an oxygen environment.</p>	<p>Liquid metal fires cannot be extinguished by normal methods. The damage of liquid metal release is real during aborts, pad emergencies or hard landings, and special fire supplements are the only method of controlling such a situation. A real credible hazard to the crew exists, which is controlled by this criterion. Indirect but immediate serious injury or death to the crew can occur via an unsuppressed fire if this criterion is not applied. The criterion is mandatory.</p>	Inspection/Test
<p><u>IR-6.</u> A nuclear payload must be maintained so as not to exceed the allowable crew dose rate.</p>	<p>Within payload bay and c.g. envelope constraints, the greater the distance, the less the dose rate that can be tolerated. This criterion is to reduce a credible (existing) hazard to the crew. Any injury received as a result of violating this criteria will lead to overdose and possible premature death. The criterion is mandatory. Standard practice is to maintain maximum possible distance and shielding sufficient to reduce the dose levels to acceptable limits.</p>	Inspection/ Demonstration

*Includes nuclear devices

Table 6-7. Ionizing Radiation (IR) Criteria (Continued)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
IR-7. Manned payload modules must be designed for rapid personnel evacuation and seal-off, if contaminated, until return to earth or decontamination can be affected, to minimize over-exposure to the crew.	This criterion is applied against a sortie payload/sortie payload subsystem. It is designed to control a credible hazard to the crew. This criterion does not completely control the hazard (see also IR-10 and IR-13). The consequence of not applying this criterion can be a direct serious injury or premature death from over-exposure; therefore, the criterion is mandatory.	Inspection/ Demonstration
IR-8. Vidicon design must eliminate radiation hazards to the crew and/or to surrounding equipments.	The amount of radiation a crew member can withstand is limited. An X-ray emitting vidicon could contribute significantly to this total. Since radiation reaching the crew is accumulating, a vidicon, which can be part of a sortie payload, poses a credible hazard to the crew. This criterion above controls this source of radiation, not all radiation. Injury to the crew would be direct in nature, and can cause permanent injury or premature death, making the criterion mandatory. Methods of X-ray control include shielding and lower voltage operation.	Test
IR-9. Redundant status monitoring and control equipment must be provided for nuclear payloads. Indication of instrument malfunction shall be included.	While the nuclear payload itself is not a hazard, it can easily become one. A malfunction instrument is a single point failure of a type which prevents the crew from knowing the condition of a controllable payload. This criterion is designed to control a credible crew hazard. Injury resulting from this hazard could be: 1) direct in nature (overdose) resulting in serious injury or premature death, or 2) indirect in nature (over temperature, sodium-potassium leak) resulting in fire and immediate injury or death. The criterion is mandatory.	Demonstration
IR-10. Payload suppliers must provide equipment for locating radioactive material which has been inadvertently released in a manned module.	Locating the released material is a prerequisite for any decontamination procedure, and must be accomplished if the crew is to/must occupy the area. This criterion is designed to allow control of a hazard (remedial measure). The hazard this would control is credible, and could cause direct crew injury or premature death if not controlled. Criteria IR-13 also is important in complete control of the hazard. This criterion is mandatory.	Inspection/ Demonstration
IR-11. Direct visual or TV coverage must be provided for nuclear isotope component transfers so as to allow the crewman to insure that the radioactive material is properly located and shielded.	This criterion is to eliminate a hazard which is credible, and if this criterion is applied, no residual hazard will exist. Any injury incurred as a result of not applying this criterion would likely be direct, with radiation causing premature death or serious injury. Indirect, delayed injury could occur if a component were simply not properly secured and shifted during reentry. The criterion is mandatory.	Demonstration

Table 6-7. Ionizing Radiation (IR) Criteria (Concluded)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
<p><u>IR-12.</u> Tracking and recovery devices must be included on nuclear payloads if, for any reason, the payload is jettisonable. Recovery of the device is to prevent dispersal of radioactivity and hazard to the populus.</p>	<p>This criterion does not directly endanger the crew. It prevents danger to the populus because of a crew action or shuttle failure. The criterion is mandatory. Tracking and recovery devices might include dye markers, beepers, and flotation gear.</p>	Demonstration
<p><u>IR-13.</u> Pressurized, manned payload modules, in which hazardous, radioactive materials are being used, must be equipped with an airlock and with radiological decontamination equipment as well as waste storage and/or disposal provisions.</p>	<p>Inability to decontaminate allows the spilled radiation to cause a continuing added source with attendant overdose to the crew. This criterion is to control a hazard (remedial action) which is credible. This criterion with IR-10 completely controls the hazard. Any injury to the crew would be direct (overexposure) and could be either serious injury or premature death. The criterion is mandatory.</p>	Inspection/Test
DISCRETIONARY		
<p><u>IR-14.</u> Nuclear reactors must not be activated while in the immediate proximity of the orbiter.</p>	<p>Activation of an RTG within the cargo bay does not in itself pose a hazard to the crew. The criteria applies to a sortie payload, but does not protect the crew from a credible hazard. The criterion is therefore discretionary.</p>	
<p><u>IR-15.</u> A reactor disposal system capability must be provided with all nuclear payloads to boost (to high-earth orbit) any damaged reactor power module.</p>	<p>Sufficient criterion have been constructed to insure minimum damage probability. If damage does occur, simple jettison would suffice to protect the crew and vehicle. Boosting to high-earth orbit is discretionary.</p>	
<p><u>IR-16.</u> Payload reactor/shield assemblies must be designed to be separable if reactor disposal in high-earth orbit is to be used.</p>	<p>Disposal of the shield with the reactor is just as acceptable to the crew. No hazard is avoided by applying the criterion. It is a cost/benefit to reuse the shield. The criterion is discretionary.</p>	
<p><u>IR-17.</u> Payloads which can be jettisoned must be ejectable through the payload bay doors.</p>	<p>Consideration must be given to such modes for contingency operation. However, this criterion does not remove a crew hazard, per se. The hazard should have been controlled by other criterion in this section. The criterion can cause another crew hazard, except on the pad. On the pad, the isotope device must be capable of withstanding an accident. This criterion is discretionary.</p>	

REPRODUCIBILITY OF THE
ORIGINAL PAGE IS POOR

Table 6-8. Contamination/Toxicity (C/T) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
<u>C/T-1.</u> To preclude inadvertent spills of hazardous fluids, payload equipment intended for use as holders, receivers, or transfer devices must have no-spill, positive-sealing characteristics.	Accidental spill of a fluid exposes the crew to the particular hazard associated with that fluid (fire, poison, acid burn, etc.). This criterion is designed to protect the crew from a credible hazard. No residual hazard exists if this criterion is applied. Direct, immediate, serious injury or death can occur from release of a hazardous fluid if this criterion is not applied. Therefore, this criterion is mandatory.	Demonstration
<u>C/T-2.</u> To minimize the effect of hazardous spills, systems must be provided for detection and collection of spilled hazardous fluids or materials.	Since many hazardous fluids can exist, and which ones are used is a function of the payload, payload equipment must sense and warn the crew of spilled, hazardous fluids. This criterion applies to subsystems of a sortie payload and is designed to protect the crew from a credible hazard. A residual hazard exists, but can be avoided by evacuation of the compartment (see C/T-5). Injury resulting from undetected hazardous fluids would be direct in nature, and can cause serious injury or death, as a function of the fluid. The criterion is mandatory.	Demonstration/ Test
<u>C/T-3.</u> Materials must not be used in habital areas of a manned spacecraft which will generate toxic or noxious fumes or dust in such concentration as to impair crew safety. (See MSCM 8080, Nos. 18, 33, 51 and 125.)	This criterion applies to the materials selection of a sortie payload and is designed to eliminate a credible hazard to the crew in the manned volume. Direct crew serious injury or death can occur from excessive levels of noxious or toxic gasses within the manned atmosphere. The criterion is mandatory. Examples include: a) un-alloyed Reryllium, b) carbon black, c) cadmium, d) polyvinyl chloride, and e) teflon wiring insulation with organic pigments. The criterion is mandatory.	Similarity/Test (For new materials)
<u>C/T-4.</u> Toxic, flammable, corrosive, or otherwise harmful fluid (or gas) containers must be located in unpressurized volumes of pressurized payloads or be double-contained such that a simple failure of the container will not expose the crew to the fluid gases.	This criterion is designed to protect the crew against a single point failure (rupture/leak of a container) which is a credible hazard. No residual hazards exist if this criterion is applied. Direct, immediate serious crew injury or death could occur should such a failure occur, releasing the hazardous gas within the manned volume. The criterion is mandatory.	Inspection/ Demonstration
<u>C/T-5.</u> If a payload operation poses risks of an explosion, fire, collision, open flame, etc., it must not be installed in the shuttle cabin which is needed for safe shuttle return.	This criterion is designed to isolate a credible crew hazard. If the shuttle cabin becomes contaminated, safe mission termination may not be possible. This causes indirect, delayed crew injury which makes the criterion mandatory.	Inspection/ Demonstration

Table 6-8. Contamination/Toxicity (C/T) Criteria (Concluded)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
<p><u>C/T-6.</u> Outgassing of payload equipment materials in vacuum must be at a sufficiently low level so as not to deposit on and obscure or damage sensitive surfaces necessary for shuttle operation. Non-availability of critical systems or surfaces (such as optics, or damaged thermal layers) may jeopardize shuttle operation, and therefore cause mission termination.</p>	<p>This criterion applies to sortie payload equipment exterior to the manned volume, and is designed to prevent a credible hazard. No residual hazard exists if this criterion is applied. Failure to apply the criteria may indirectly affect the crew by causing the inability of the vehicle to operate properly, possibly causing inability to terminate the mission. The criterion is therefore mandatory.</p>	Similarity/Test
<p><u>C/T-7.</u> Critical close-tolerance systems must be adequately protected from particulate contamination to prevent loss of the fluid system with consequent hardware failure which could propagate to crew hazards.</p>	<p>This criterion is to protect the crew against loss of a critical system from particulate matter. This credible hazard is controlled by this criterion. Injury from loss of a system can be direct (such as the environment control system) or indirect. Indirect injury can be either delayed or immediate, and serious injury or loss of life could occur by any of the three avenues, making the criterion mandatory. Normal design procedure includes filters and provisions for flushing the system.</p>	Inspection
<p><u>C/T-8.</u> Packing of pathogenic containers must be capable of withstanding off-nominal landings to protect the crew and ground personnel from exposure.</p>	<p>This criterion protects personnel from a credible exposure hazard. No residual hazard exists if this criterion is applied. Direct, serious injury or death from the disease could occur if the container were to burst and expose personnel, making the criterion mandatory.</p>	Analysis/Test
<p><u>C/T-9.</u> Payloads containing pathogenic, microbiological or biological experiments must be compartmented to isolate such organisms from human contact during ground and flight operations in order to protect the health and safety of the crews.</p>	<p>This criterion will preclude a credible crew hazard from occurring, that of exposure to harmful microbes. No residual hazard exists if this criterion is applied. Failure to apply this criterion would allow exposure of the crew to hazardous microbes, with the possibility of direct, immediate, serious injury or death resulting. Thus, the criterion is mandatory.</p>	Demonstration/Test

Table 6-9. Fire (F) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
F-1. Flammable or explosive material within TBD feet of the single entrance to a compartment must not, if accidentally released, preclude shirt sleeve access through the entrance, thus trapping the occupants.	This criterion protects the crew from a credible hazard associated with energy release. No residual hazard exists if this criterion is applied. If this criterion were not applied, direct injury by the material release could occur to occupants of a compartment, causing serious injury or death to a crew member. This makes the criterion mandatory.	Analysis
F-2. Payload materials used within the manned volume must be designed to the same flammability constraints as the orbiter. Where the nature of an experiment involves a combustible process, it must be isolated by payload equipment. Fire prevention within the cabin, at least to the level of orbiter design, is required to protect the crew. (See MSCM 8080, No. 22.)	This criterion is to protect the crew from an unacceptable level of fire hazard. The hazard is credible, and no residual hazard exists if this criterion is applied. The occurrence of fire within the manned volume creates the possibility of direct, serious injury or death to the crew. Thus, the criterion is mandatory.	Inspection/Test
F-3. Equipment containing hot surfaces (in excess of TBD °F) must be isolated so as not to be a source of ignition for flammable materials within the manned volume.	This criterion is to protect the vehicle/crew from fire on the shuttle, a credible hazard. No residual hazard exists from this ignition source if this criterion is applied. If an ignition were to occur within the manned volume, direct, serious injury or death could occur from the sustained fire. If an ignition were to occur exterior to the manned volume, indirect, serious injury or death can occur either immediately, due to propagation of the fire, or delayed because of inability to enter as a result of vehicle damage. The criterion is mandatory.	Analysis/ Demonstration
F-4. Potential ignition sources in the payload (such as switches and relays) must be contained so as to prevent open arc or spark generation.	The criterion applies to subsystems of a sortie payload, and is designed to protect the crew from a credible fire hazard. No residual hazard exists if this criterion is applied. Within a manned volume, failure to apply this criterion allows available ignition sources which can ignite a combustible, causing indirect but immediate crew serious injury or death from the fire. The criterion is mandatory.	Inspection
F-5. Exhaust producing hot gas systems must not be used by payloads. Hot gas exhaust by-products, and/or the flame itself, can damage the payload bay area or cause secondary fires within the bay.	The criterion applies to a sortie payload subsystem (mounting/jettison capability), and is designed to protect the vehicle and crew from a credible hazard, which is completely controlled by this criterion. Indirect, immediate, serious injury or death can occur, if this criteria is not applied, as a result of a fire onboard. Indirect, delayed inability to safely terminate the mission can also occur if damage to the payload bay/doors could cause aerodynamic instability upon entry. The criterion is mandatory. Jettison can be accomplished by closed, hot gas systems, or kinetic energy methods such as springs.	Inspection

REPRODUCIBILITY OF THE
 ORIGINAL PAGE IS POOR

Table 6-9. Fire (F) Criteria (Concluded)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
F-6. To preclude uncontrollable fires, payloads which introduce extraordinary or unusual fire hazards must supply the necessary suppression equipment.	This criterion protects the crew from a credible fire hazard. No residual hazard exists if this criterion is applied. If in the manned volume, failure to apply this criterion allows possibility of fire with direct, serious injury or death of the crew member occurring. Exterior to the manned volume, failure to apply this criterion indirectly jeopardizes the crew by allowing possibility of fire and vehicle damage, preventing safe mission termination; or if the fire propagates to the manned volume, immediate, serious injury. In either case, the criterion is mandatory.	Inspection
F-7. A manned payload module must have both manually (local) and remotely controlled means of fire suppression and control. Local control of small blazes, or remote control of a fire which forces evacuation of the compartment are necessary to control the possibility of crew injury.	This criterion protects the crew from a credible hazard. E/I-18 supplies life support to help the crew escape the fire should that be necessary. This minimizes the residual hazard. When the manned module is occupied, direct, serious injury or death could occur as a result of an unsuppressed fire. When the manned module is not occupied, inability to remotely extinguish a fire will allow serious consequences, possible propagation to the vehicle cabin resulting in indirect, immediate serious injury or death to the crew. The criterion is mandatory.	Inspection
F-8. Capability must be provided to automatically shut off air circulation fans in a manned payload module upon detection of a fire within that module for purposes of fire control and containment.	This criterion is levied against a sortie payload subsystem, and is designed to protect the crew from a credible hazard of fire. The hazard of lack of life support is covered by E/I-18, and extinguishing the fire by F-7. If this criterion is not applied, the oxidizer needed for support of the fire will not be removed, and indirect but immediate serious injury or death can occur. Thus, the criterion is mandatory.	Demonstration
DISCRETIONARY		
F-9. Payload instrumentation and command links must be protected from open fire to insure control capability of payloads.	This criterion is levied against a sortie payload, and is designed to protect the crew from a hazard, loss of payload control. However, the hazard is not a credible hazard, as open flame is not allowed, and other criteria are to prevent accidental fires, leaving the criterion discretionary.	

Table 6-10. Fuels and Oxidizers (F/O) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
<p>F/O-1. To preclude the possibility of fires or explosion, payload cryogenic fuels and oxidizer systems must be designed to preclude accumulation or mixing of the combustibles in any unintended location.</p>	<p>Accumulation of fuels/oxidizers can cause fire hazard; accumulations which mix can cause danger of explosion or fire. This criterion controls this particular hazard. There is no residual hazard. Any injury to the crew from occurrence of this hazard would be indirect in nature, with a fire/explosion damaging the vehicle. Immediate serious injury or death could occur from propagation of the fire; indirect delayed inability to safely deorbit could occur if damage to the vehicle was exterior. The criterion is mandatory.</p>	<p>Inspection</p>
<p>F/O-2. Cleanliness requirements for fuel and oxidizer systems must be consistent with shuttle cleanliness requirements. Contaminants in such systems can form explosive combinations.</p>	<p>This criterion protects the vehicle and crew from a credible explosive hazard. Indirect, immediate serious injury or death can occur from these explosive combinations detonating and the resultant fire propagating to the manned volume. The criterion is mandatory.</p>	<p>Inspection</p>

Table 6-11. Pressure Vessel (PV) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
PV-1. Redundant venting provisions must be provided on cryogenic and hydrogen peroxide systems which have pressure buildup in normal conditions.	This criterion is to protect the vehicle and crew from a credible hazard (overpressure). No residual hazard exists if this criterion is applied. Injury to the crew would be indirect in nature, where the overpressure release would affect the vehicle, and crew members could experience immediate serious injury or death from pressure damage or uncontrolled motion due to propulsive venting. The criterion is mandatory. Secondary relief valves or burst disks are normal design.	Inspection
PV-2. Regulator shutoff valve design must include extremes for temperatures such as the consequence of flow through a stuck-open regulator. An inoperable shutoff valve exposes downstream equipment to over-pressure action.	This criterion is to protect the crew from a credible hazard. Occurrence of this hazard can directly affect the crew, causing death or serious injury when the environment control system is involved, or the equipment explodes in the manned volume. Indirect, immediate serious injury can also occur if the regulator sticks and resultant explosion does damage to the vehicle. The criterion is therefore mandatory.	Test
PV-3. For all payload equipment requiring an operative vent, equipment operation must be prevented in the event of vent system malfunction to preclude critical over-pressurization of the vent system.	This criterion is to protect the crew member from a credible hazard. If operation were to take place under these conditions, over-pressure and explosion of the vent line could result; direct crew injury would result. Injury occurring as a result of this hazard would be direct in nature with the over-pressured line exploding and fragments injuring the crew member. The criterion is therefore mandatory.	Demonstration
PV-4. Each payload pressure system must have a relief capability; however, any venting into the payload bay must not exceed the bay venting capability with the payload bay doors closed.	Relief capability is to prevent explosion; vent restriction is to prevent over-pressure damage to the orbiter. This criterion is designed to prevent these hazards, which are credible. If this criterion is applied, there is no residual hazard. Any injury to the crew as a result of not applying this criterion would be indirect in nature, with the most likely situation being damage to the vehicle of such a nature that safe termination would not be possible. The criterion is mandatory.	Analysis
PV-5. High pressure gas lines and vent lines must be secured to preclude a line rupture from producing line whipping with consequent damage to the vehicle or injury to a crew member.	This criterion, if applied, protects the crew from a credible hazard. This criterion will control the hazard and any crew injury will be indirect in nature, most likely by making the vehicle unsafe for mission termination. The criterion is therefore mandatory.	Analysis/ Inspection

Table 6-11. Pressure Vessel (PV) Criteria (Continued)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
PV-6. Components that are sensitive to fluctuations in supply pressure must be designed so that their failure mode does not violate the system pressure integrity. Release of the pressurized fluid constitutes a hazard to vehicle/crew as well as other payloads. Hazardous fluids can cause a direct hazard; other fluids cause a propulsive vent (payload bay) or over-pressure of manned volume.	This criterion is to protect the crew from source credible pressure source hazards. Direct crew injury or death could occur if the pressure is vented into the manned volume or if a fire can occur. Indirect crew injury can occur if venting in the payload bay causes propulsive effects. The criterion is mandatory.	Test
PV-7. Payload battery cases must be capable of withstanding worst case over-pressures without rupturing.	This criterion applies and the hazard being controlled presents a credible hazard to the crew. There is another criterion (ESI-1) which contributes to complete control. Without this criterion, direct crew serious injury or death could occur if the battery were in a manned module. Indirect immediate serious injury could occur if the battery were external to the manned volume. The criterion is mandatory.	Test
PV-8. Payload equipment in a manned volume must be designed to withstand a rapid decompression without causing a hazardous condition such as exploding or allowing flying objects to be in the manned volume. (See MSCM 8080, No. 2.)	This criterion applies and is designed to prevent a credible crew hazard from occurring. Direct, immediate, serious crew injury or death could be caused by the results of an "explosion" of equipment during decompression. The criterion is therefore mandatory.	Test
PV-9. All hazardous fluid or gaseous system valves must be completely operable with either an upstream or a downstream pressure differential equal to the maximum system pressure. Any valve can be called upon to shut off a section of line because of breakage and prevent dumping the fluid. A vented or dumped hazardous fluid endangers the crew directly or indirectly.	This criterion is designed to protect the crew from a credible hazard. If the lines/valves were in a manned volume, or part of the environment control system, direct, immediate, serious injury or death could occur. If the lines/valves were outside the manned volume, fire and indirect, immediate injury is possible. The criterion is mandatory.	Demonstration/ Test
PV-10. Fluid and vacuum lines penetrating a manned payload module must meet all the design criteria of the main pressurized volume. Protective systems must be designed with the capability to protect against failure of the largest penetration.	This criterion is to prevent a failure of a line which could act to vent the manned sortie module to space or release a fluid into the module. This criterion applies and is designed to protect the crew from a credible hazard. Should either a release of fluid or a vent occur, direct injury to the crew could occur and would be immediate, with possibility of serious injury or death occurring. The criterion is therefore mandatory.	Test

Table 6-11. Pressure Vessel (PV) Criteria (Continued)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
PV-11. Differential pressure gauges must be designed so that the high and low pressure sensing connectors cannot be physically interchanged. Loss of the gauge or a burst diagram within the gauge present hazards to the crew.	On some systems the loss of a differential pressure gauge would allow hazards to go uncorrected. Venting any hazardous gas into the cabin from a burst gauge also poses a direct hazard to the crew. This criterion is designed to protect the crew from credible hazards. No residual hazard exists if this criterion is levied. Direct, serious injury or death could occur if this criterion were not levied and gas vented into the cabin. Indirect, immediate, serious injury or death could occur if a preventable malfunction occurred because of instrumentation. In either case, the criterion is mandatory.	Inspection
PV-12. Payload tank and pressure vessel design safety factors must be at least as conservative as the orbiter safety factors to insure against loss of the vessel and inherent vehicle damage or crew injury.	This criterion is designed to protect the crew from a credible over-pressure hazard. Failure of pressure vessels, within the manned volume, could cause direct, immediate crew serious injury or death should over-pressure explosion occur. Pressure vessels outside the manned volume exploding could cause vehicle damage making safe termination impossible. The criterion is mandatory.	Analysis
PV-13. Pressure vessels and/or lines that cannot meet at least the orbiter safety factor, must be protected so that personnel cannot cause damage, and thus lower the safety factor of the vessels while working on or near these components.	This criterion is to protect the crew from a credible hazard. No residual hazard will occur if this criterion is applied. If the pressure vessel is within the manned volume, failure of the vessel can cause direct, serious injury or death to the crew member by venting a hazardous fluid or from over-pressure. If the pressure vessel is exterior to the manned volume, failure of the vessel can cause damage to the aerodynamic capabilities of the vehicle, preventing safe mission termination. It should be noted that failure would not necessarily occur when damage occurs; failure could occur at next pressurization. In either case, the criterion is mandatory.	Inspection
PV-14. Capability shall be provided for the orbiter crew to dump hazardous payload fluids and gases overboard within the time constraints imposed by an abort situation so the fluids cannot be released on impact/loading and cause crew injury, and with the payload doors opened or closed. Dumping techniques must preclude mutually reactive fluids from mixing and resulting in a fire or explosion.	This criterion applies to a sortie payload subsystem (hydrazine, oxygen, etc.) and is designed to protect the crew from a credible hazard of fire/explosion on impact/landing. No residual hazard exists if this criterion is applied. Injury as a result of this hazard could be either direct or indirect, but would be immediate in nature with serious injury or death resulting from fire/explosion. Thus, the criterion is mandatory.	Inspection

Table 6-11. Pressure Vessel (PV) Criteria (Continued)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
DISCRETIONARY		
<u>PV-15.</u> Venting from a pressure vessel must be non-propulsive to preclude motion and off-balance crew injury.	This criterion does not protect the crew from a credible injury hazard. Indirect injury could occur as a result of unanticipated vehicle motion if venting is propulsive in nature, but venting impulse versus the shuttle dynamics will not allow significant motion to occur. Thus, the criterion is discretionary.	
<u>PV-16.</u> A reservoir must be incorporated prior to a vent terminus to permit required system venting during critical operational periods without the corresponding propulsive forces and contamination around the orbiter.	Since venting impulse is non-propulsive in nature, no credible crew hazard can occur from allowing the venting to occur. This is a mission success criterion statement. This criterion can be applied to a sortie payload subsystem, but does not protect the crew from a credible hazard. The criterion is discretionary.	
<u>PV-17.</u> Quick-disconnects to vacuum must be avoided for critical functions to preclude leaks.	The only hazard involved with the use of quick-disconnects is leakage. (Wrong connectors have already been precluded.) The reliability of currently approved quick-disconnects and the application (plumbing with vent valving) precludes dangerous leakage. The residual leakage hazard is not credible. The criterion is discretionary.	
<u>PV-18.</u> When one pressure source supplies multiple demands, worst case design demands must be taken into account so that required pressures are maintained.	Insufficient supply could cause a payload to fail. However, any failure which could injure the crew should be precluded by existing criteria, and the under-pressure will not in itself cause danger to the crew. Though this criterion can be applied to a sortie payload, it does not present a credible hazard to the crew if not applied to the payload. The criterion is discretionary.	
<u>PV-19.</u> All payload systems using hydrogen peroxide must be designed to permit accurate determination of the rate of active-oxygen loss from the hydrogen peroxide. (See MSCM 8080, No. 44.)	Any use of hydrogen peroxide on the payload would be functional in nature, and not a system upon which the crew would be dependent. Depletion of the hydrogen peroxide would terminate the experiment, but would not generate a credible crew hazard. Pressure and temperature considerations have been treated elsewhere. Thus, the criterion is discretionary.	
<u>PV-20.</u> Where small safety factors are involved (e.g. <2), capability must be provided to measure the parameter(s) required to detect potential pressure vessel failures.	Detecting pressure vessel failure may allow some crew action to protect vehicle/crew (such as manual venting); however, venting, burst disks, etc., already preclude pressure vessel failure from over-pressure and impact failure is also precluded. Thus, this criterion is redundant to others, and does not protect the crew from a credible hazard, leaving the criterion as discretionary.	

Table 6-11. Pressure Vessel (PV) Criteria (Concluded)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
DISCRETIONARY		
<p>PV-21. Gaseous content of payload pressure vessels with necessarily low safety factors (<TBD) must be small enough so that rapid isentropic expansion will not result in a hazardous over-pressure.</p>	<p>This criterion is designed to protect the crew and vehicle should a pressure vessel fail. Relief venting is required to prevent any over-pressure situations from occurring. The only remaining hazard, then, is a fatigue type failure, and the chances of this occurring are not credible. Although the criterion can be levied on a sortie payload, and is designed to protect the crew, the hazard being eliminated is not credible. Thus, the criterion is discretionary.</p>	
<p>PV-22. Pressure vessels with critically low safety factors (<TBD) must be of shrapnel-proof design or be provided with shrapnel-proof barriers.</p>	<p>This criterion is designed to prevent shrapnel damage when a vessel bursts. However, since vent provisions are required, the vessel will not burst and the hazard is not credible. The criterion is therefore discretionary.</p>	

Table 6-12. Structural (S) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
S-1. All rotating components must be designed to preclude fragmentation damage to the vehicle or injury to the crew.	This criterion prevents the occurrence of a credible crew hazard. This criterion controls this hazard. There is no residual. If fragmentation were to occur within the manned volume, shrapnel could cause serious injury or death directly, and immediately. If fragmentation occurs exterior to the manned volume, serious damage can occur to the vehicle, making safe mission termination impossible. The criterion is mandatory.	Analysis/Test
S-2. Any payload deployment system must provide positive control of the payload movements and preclude permanent violation of the payload bay envelope.	Uncontrolled motion of part of the payload allows impact with, and damage to, the vehicle. Inability to remedy a violation of the payload bay envelope precludes closing of the doors, and prevents reentry. This criteria applies to the subsystems of a sortie payload, and is designed to eliminate a credible crew hazard. If this hazard were allowed to occur, indirect injury or death can occur to the crew (delayed) because of an inability to safely deorbit. The criterion is mandatory. Stiffness of supports, fail operational/fail-safe and jettison mechanisms are design techniques to preclude these hazards.	Demonstration
S-3. A safety factor of TBD (referenced to worst case loads) must be provided all mechanical fasteners used to lock or secure a payload component.	This criterion applies to a sortie payload subsystem (mounting) and is designed to prevent a credible crew hazard. No residual hazard will occur if this criterion is applied. If a fastener or mount breaks loose within the manned volume, direct, serious injury or death can be caused by the flying object. If a fastener or mount breaks loose outside the manned volume, exterior damage to the vehicle can occur which will prevent safe entry. The criterion is mandatory.	Analysis/Test
S-4. Any payload using portable containers must insure restraint of the containers when not in use to preclude loose object damage to vehicle or injury to crew.	This criterion prevents a credible crew hazard from flying objects. No residual hazard occurs if this criterion is applied. Unsecured containers flying about the manned volume can cause direct, serious injury or death to a crew member by striking him. The criterion is therefore mandatory.	Inspection
S-5. Payloads must not be dependent on internal pressures for structural integrity if the shuttle vehicle could be damaged by loss of the pressure (integrity).	This criterion controls a credible hazard; no residual hazard occurs if this criterion is applied. Damage to the vehicle could be of a nature which would prevent safe entry (such as payload bay door damage). This would cause an indirect, delayed hazard to the crew, making the criterion mandatory.	Analysis/Test
S-6. Manned, pressurized volumes must be designed to operate within the meteoroid environment defined in NASA SP-8013, dated March 1969, to prevent crew injury from sudden loss of atmosphere due to meteoroid impact. (See MSCM 8080, No. 21.)	This criterion protects the crew from a credible hazard. No residual hazard exists if this criterion is applied. Direct, serious injury or death could occur if this criterion is not applied, from sudden depressurization. The criterion is therefore mandatory.	Test

Table 6-12. Structural (S) Criteria (Concluded)

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
DISCRETIONARY		
<p>S-7. Payload equipment which extends outside the payload bay must be so located as to not interfere with docking.</p> <p>S-8. Outer pressure walls of a manned payload module must be accessible so pressure leaks can be located and repaired.</p>	<p>This criterion can be levied against a sortie payload, but does not protect the crew against a credible hazard. Normal interference of payload/docking can be avoided by mission timeline; a stuck-up payload can (and will) be jettisoned; and the payload can be lowered to facilitate emergency docking. Thus, there is no credible hazard, and the criterion is discretionary.</p> <p>This criterion can be levied against a sortie payload, but does not protect the crew from a credible hazard. S-6 requires the possibility of puncture to be designed out, per NASA SP-8013; and even if this low risk incident should occur, the module can be evacuated using portable life support equipment, required by E/I-18, and sealed off. This design criterion is for mission success, and is discretionary.</p>	

Table 6-13. Systems Interactions (SI) Criteria

DESIGN CRITERION	CATEGORIZING RATIONALE	VERIFICATION
MANDATORY		
SI-1. Safety status payload signals must be provided for crew display to allow control of payload hazards.	This criterion requires warning the crew of a hazard where control can be exercised over the hazard. The hazard is credible, and no residual hazard exists if this criterion is applied (it is controlled). Within the manned volume, direct serious injury or death can occur from an uncontrolled hazard. Exterior to the manned volume, payload hazards can damage the vehicle, allowing indirect, immediate, serious injury or delayed inability to re-enter. The criterion is mandatory.	Inspection
SI-2. Automatic event-sequencing programs must be capable of initiation only when commanded by a crew member or ground control if vehicle damage or crew injury could occur from unplanned operation.	This criterion protects the crew from a credible hazard of inadvertent operation. No residual hazard occurs if this criterion is applied. Inadvertent operation within a manned volume can cause direct, serious injury to the crew member. Inadvertent operation exterior to the manned volume can cause damage to the vehicle which will make reentry unsafe (such as an extension boom extending prior to the bay doors being opened). In either case, the criterion is mandatory.	Inspection
SI-3. A single-signal malfunction must not generate a signal which could result in premature initiation of subsequent sequences.	This criterion is to preclude a credible hazard, inadvertent initiation of sequences which may be remedial in nature. Such sequences initiated in an untimely manner can cause hazardous situations, or expend safety measures. The result can be indirect, immediate crew injury (by motion from venting, etc.) or delayed, caused by inability to enter, making the criterion mandatory.	Inspection
SI-4. A single instrumentation failure must not inhibit an automatic warning system from monitoring other functions.	This criterion controls a credible hazard which can impact the crew. The occurrence of one instrument indication or malfunction must not allow another malfunction to go undetected, or crew injury can result, either directly or indirectly, as a function of the systems being monitored. The criterion is mandatory.	Inspection/ Demonstration
SI-5. Provisions must be made for verifying critical payload systems readiness before placing it on line. A critical system not configured for bringing on the line can react in a manner to cause a hazard.	Bringing an improperly configured system on line can cause a credible crew hazard. This hazard is controlled by this criterion. The equipment or system could react in a manner to cause either direct or indirect crew injury, depending on the system and its location. The criterion is mandatory.	Inspection

REPRODUCIBILITY OF THE
ORIGINAL PAGE IS POOR

Table 6-14. Subsystems Cross Reference

SYSTEM/INTERFACE AREA	SAFETY STUDY HAZARD AREAS											
	EXPLOSIVE DEVICES	ELECTRIC SHOCK	ENERGY SOURCE ISOLATION	EXT/INT VEHICULAR ACTIVITY	MATERIALS COMPATIBILITY	IONIZING RADIATION	CONTAMINATION/TOXICITY	FIRE	FUELS & OXIDIZERS	PRESSURE VESSELS	STRUCTURAL	SYSTEMS INTERACTIONS
	(ED)	(ES)	(ESI)	(E/I)	(MC)	(IR)	(C/T)	(F)	(F/O)	(PV)	(S)	(SI)
	APPLICABLE CRITERIA NUMBERS*											
COMMUNICATIONS	--	1-3	12	18,19	3	11,12	3,6	3,4,9	--	--	--	2
CRYOGENICS	--	--	21	1,9,11,15	2-4	3	1-8	1,3,5-7	1,2	1-22	--	5
DATA PROCESSING & SOFTWARE	--	1-3	12,15	5,10	3	--	3	3,4,9	--	--	--	1-5
DISPLAYS & CONTROLS	--	1-3	15	2-5,8-15, 18,20,21	3	3,5,7-11, 13,15	2,3,5-7	3,4,7-9	--	1-3,9-11, 14,19	2	1-5
ELECTRICAL POWER	2-7,10	1-3	1-20	13,15,16, 18,19	2,3	5,7-11, 13-15	2,3,5-7	1,3-9	--	2,3,7,9,10, 17	--	1-5
ENVIRONMENTAL CONTROL & LIFE SUPPORT	--	--	13,21	1,8,11,15, 16,18,19	2-4	7,13	2-5,7,8	1,3,4,6-8	1,2	1-22	5	--
EXT/INT VEHICULAR ACTIVITY	9	--	--	1-22	2	1-17	2,3,5,7	1,7	--	13,14	1,3,8	2,5
INSTRUMENTATION	--	1-3	12,15	2,5,8,10, 12,16-19	2,3	3,5,7,9-13, 15	2,3,5,6	3,4,7-9	--	3,9-11,14, 19,20	--	1-5
ONBOARD CHECKOUT	--	--	--	2,11,12,20	3	4,9,11,13	2,3,5,7	3,4	--	--	--	1-5
PAYLOAD ENVIRONMENT	9	--	10,17,21	1,8,11, 14-22	2-4	1,3-5,7,8, 10,13	2-6,8,9	1,3,7	1,2	8,9	--	--
PYROTECHNICS	1-10	--	--	15,17,19	3	15	5,6	1,3-6	--	--	2	--
STRUCTURES	--	2	3,4,14	6,7,9,12,14, 15,17-22	1-4	1,3-7,11, 13,15-17	1,3,4,6,8,9	1,3-7,9	1,2	1-22	1-8	--
THERMAL CONTROL	--	--	1,5,13,18, 21	1,11,15	2,3	1,2,4,5	3,6,7	3,4,6	1,2	2,9	--	--

*Listed in Tables 6-2 through 6-13

22214-H014-RO-00

7. CONCLUSIONS

During the course of this study, several points were noted that might be useful to NASA/JSC in implementation of requirements in the Shuttle era.

7.1 STUDY RESULTS

The results of this study will form the basis for detailed payload specifications to be written when quantitative shuttle data is available. Utilization of the mandatory design criteria will help assure that future shuttle sortie payloads insure the safety of the space shuttle vehicle and crew. Since Shuttle Program management will concentrate only on those criteria and specifications considered mandatory, considerable cost savings can be realized by reduced manpower, less need for Shuttle Program managerial cognizance over certain criteria, and less paperwork. Also, when new criteria are generated due to changes in subsystems, designs, or guidelines used by this study, the categorization process can be used to aid in managerial decision-making concerning the new criteria.

7.2 PROGRAM OFFICES

In past programs, frequently the same program office was responsible for payloads (experiments) and spacecraft development. This philosophy lends itself to working out design problems by modification of both the payload and spacecraft. This type working situation will not be practical in the shuttle era since the vehicle should not be modified for each successive payload. This working situation also leads to the payloads being designed and qualified to the same standards as the vehicle which is an expensive practice not necessarily in harmony with shuttle era philosophies.

7.3 SYSTEMS SAFETY DESIGN CRITERIA CATEGORIES

It is a conclusion of this study that two separate sets of systems safety criteria should be applied to payloads in general.

Safety criteria are necessary to provide crew/shuttle safety from the payloads. The criteria in this volume relate to crew safety from sortie payload hazards.

The discretionary criteria in this volume pertain to mission success for the payload, and are implemented at the option of the payload integrator

or developer. However, the payload user may decide that these discretionary criteria may be mandatory to assure success of the payload.

7.4 SAFETY REQUIREMENTS AND GUIDELINES

The NASA/JSC Safety Office has produced a substantial set of safety requirements and guidelines. When a hardware contract is let, safety requirements are usually levied as part of the contract in addition to a requirement for a hazard analysis. Once a thorough hazards analysis has been performed for a type of equipment, subsequent hazards analyses are replotting old ground, except where new technology is being created on a particular piece of hardware. If JSC were to compile the accumulation of available safety requirements and guidelines into one source document, JSC could more effectively levy a complete set of safety requirements and eliminate the need for repetitive, detailed hazards analyses except where new technology is being implemented.

7.5 HARDWARE SAFETY

This study emphasized crew safety, with consideration given to vehicle hardware safety where vehicle damage could propagate into crew injury. For other systems safety criteria, the systems compatibility report (volume III) needs to be taken into consideration.

REFERENCES

1. "Apollo Test Requirements," NHB 8080.1, NASA OMSF, March 1967.
2. "Safety Program Directive No. 1-Revision A (SPD-1A)," 1700.120, NASA/OMSF, 12 December 1969.
3. "Preliminary Hazard Analysis of Space Shuttle Payloads and Payload Interfaces," MSC 06815, NASA/MSC, April 1972 (Preliminary).
4. "Safety in Earth Orbit Study," Final Report, MSC-04477, (North American Rockwell, SD 72-SA-0094-5), NASA/MSC, 12 July 1972.
5. "Advanced Missions Safety," ATR-72(7316-01)-1, Aerospace Corporation, 15 October 1972.
6. "Systems Safety Guidelines of New Space Operations Concepts," LMSC-A968322, MSFC, Lockheed Missiles and Space Company.
7. "Manned Space Flight Nuclear System Safety," 725D 4201-5-2, General Electric, January 1972.
8. "Manned Spacecraft Criteria and Standards," MSCM 8080, Change 4, NASA/MSC, 21 April 1972.
9. "Space Flight Hazards Catalog," MSC 00134, Revision A, NASA/MSC, January 1970.
10. "Space Vehicle Operational Design Criteria Manual," MSC 04969, Volume I, NASA/MSC, 1 December 1971.
11. "Radiation Protection Guides and Constraints for Space-Mission and Vehicle-Design Studies Involving Nuclear Systems," Committee on Space Medicine, Radiobiological Advisory Panel, Space Science Board of the National Academy of Sciences, 1970.
12. "Standard Satellite System Safety Design Criteria," USAF/SAMSO, 10 February 1972.
13. "Systems Safety," AFSC DH 1-6, USAF/AFSC, 10 January 1972.
14. "Space Shuttle Baseline Accommodations for Payloads," MSC 06900, NASA/MSC, 27 June 1972.
15. "Reference Earth Orbital Search and Applications Investigations (Blue Book)," NHB 7150.1, NASA, Volumes I through VIII, January 1971.

BIBLIOGRAPHY

- "Advanced Missions Safety," ATR-72(7316-01)-1, Aerospace Corporation, 15 October 1972.
- "Apollo Applications Program Experiment Hardware General Requirements," MSC-KA-D-68-1, Revision B, NASA/MSC, 27 January 1970.
- "Apollo Spacecraft Nonmetallic Material Requirements," PA-D-67-B, NASA/MSC, February 1968.
- "Apollo Test Requirements," NHB 8080.1, NASA/OMSF, March 1967.
- "Basic Safety Requirements," NHB 1700.1, Volume VI, NASA, July 1969.
- "Centaur Payload User's Manual," NASA CR-72109, General Dynamics Convair Division, August 1966.
- "Checklist of General Design Criteria," AFSC DH 1-X, USAF/AFSC, 15 January 1970.
- "Delta Payload Planner's Guide," McDonnell Douglas, Rev. June 1970.
- "Design Requirements for Shuttle Payloads," NASA Memo from Dale D. Myers to Philip E. Culbertson, 23 February 1973.
- "Electromagnetic Compatibility Requirements MOL System Orbiting Vehicle," TOR-0200 (4107-28)-2, Aerospace Corporation, June 1968.
- "Flammability, Odor, and Offgassing Requirements and Test Procedure for Materials in Environments That Support Combustion," NHB 8060.1, NASA, November 1961.
- "Gemini B Oxygen Safety Study, Volume VII, Simplified Two Gas System," F415, McDonnell Astronautics Company, 19 May 1967.
- "General Requirements for Hardware Procurement," D2-118444-1, Boeing, 21 July 1972.
- "HEAO System Safety Requirements Document," Contract No. NAS 8-26273, TRW, 23 April 1971.

BIBLIOGRAPHY (Continued)

- "Ionizing Radiation Control," AFETRM 160-1, USAF/AFETR, 20 September 1972.
- "Manned Safety Assessment of MSC Experiments, Design Certification Review," Volume VII, Section III, NASA/MSC.
- "Manned Spacecraft Criteria and Standards," MSCM 8080, NASA/MSC, 26 April 1971.
- "Manned Space Flight Nuclear System Safety," 725D 4201-5-2, General Electric, January 1972.
- "Military Standardization Handbook, Metallic Materials and Elements for Aerospace Vehicle Structures," MIL-HDBK-5B, DOD, 1 September 1971.
- "MOL Ground Test Plan, Acceptance Test Plan, Volume I, AVE Components Through Subsystems and AGE CEI's," DAC-57179, Douglas, 25 June 1968.
- "MOL Program Detailed Test Plan for Material Properties," TOR-1001 (2107-30)-4, Aerospace Corporation, December 1966.
- "MOL Program Structural Criteria for the Laboratory Vehicle Segment," TOR-1001 (2107-30)-3, Aerospace Corporation, December 1966.
- "MSC Guidelines for Establishing Safety Requirements for Space Flight Contractors" (Preliminary), MSCM1702, NASA/MSC, July 1972.
- "NASA CV-990 Laboratory Experimenters' Handbook," NASA/ARC, November 1970.
- "Particles and Fields Subsatellite Project, System Hazard Analysis," 2260.1 4-34, TRW, 14 July 1970.
- "Preliminary Hazard Analysis of Space Shuttle Payloads and Payload Interfaces," MSC 06815, NASA/MSC, April 1972, (Preliminary).
- "Procedures and Requirements for the Flammability and Offgassing Evaluation of Manned Spacecraft Nonmetallic Material," D-NA-0002, NASA/MSC, July 1968.

BIBLIOGRAPHY (Continued)

- "Radiation Protection Guides and Constraints for Space-Mission and Vehicle-Design Studies Involving Nuclear Systems," Committee on Space Medicine, Radiobiological Advisory Panel, Space Science Board of the National Academy of Sciences, 1970.
- "Range Safety Manual," AFETRM 127-1, USAF/AFETR, 1 September 1972.
- "Reference Earth Orbital Search and Applications Investigations (Blue Book)," NHB 7150.1, NASA, January 1971.
- "Research and Applications Modules (RAM) Phase B Study," GDCA-DDA72-006, General Dynamics, 12 May 1972.
- "Safety In Earth Orbit Study," MSC-04477, (North American Rockwell SD 72-SA-0094-5), NASA/MS, 12 July 1972.
- "Safety Plans, Programs, and Procedures," SAMSOM 127-1, Volume IV, USAF/SAMSO, 14 August 1970.
- "Safety Program Directive No. 1-Revision A (SPD-1A)," 1700.120, NASA/OMSF, 12 December 1969.
- "Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program," NHB 5300.4(1D), NASA, December 1972.
- "Shuttle Orbiter/Payloads Monitor and Control Interface Study," SD72-SA-0043, North American Rockwell, 1 May 1972.
- "Skylab System Safety Checklist Experiment Ground Support Equipment Design," SA-003-004-2H, NASA/MSFC, November 1971.
- "Skylab System Safety Checklist Experiment Systems Design," SA-003-003-2H, NASA/MSFC, November 1971.
- "Skylab System Safety Checklist Ground Support Equipment Design," SA-003-001-2H, NASA/MSFC, July 1971.
- "Sortie Laboratory Guidelines and Constraints Level 1," NASA, 15 August 1972.

BIBLIOGRAPHY (Concluded)

- "Space Flight Hazards Catalog," MSC 00134, Revision A, NASA/MSC, January 1970.
- "Space Shuttle Baseline Accommodations for Payloads," MSC 06900, NASA/MSC, 27 June 1972.
- "Space Shuttle EVA/IVA Support Equipment Requirements Study Presentation," Contract No. NAS 9-12506, Hamilton Standard, 14 June 1972.
- "Space Shuttle Science Instrument Development Studies," JPL Job No. 612-50101-0-823, Jet Propulsion Laboratory, 18 September 1972.
- "Space Station Program Phase B Definition," MSC-00737, (North American Rockwell/SD 70-145), NASA/MSC, 13 March 1970.
- "Space Vehicle Operational Design Criteria Manual," MSC 04969, Volume I, NASA/MSC, 1 December 1971.
- "Standard General Requirements for Safe Design and Operation of Pressurized Missile and Space Systems," MIL-STD-1522, DOD, 1 July 1972.
- "Standard Satellite System Safety Design Criteria," USAF/SAMSO, 10 February 1972.
- "Study of Space Shuttle EVA/IVA Support Requirements," Vought Missiles and Space Company, 15 June 1972.
- "Systems Safety," AFSC DH 1-6, USAF/AFSC, 10 January 1972.
- "System Safety Checklist, EREP Tape Recorder Breakout Box," (MMC SK840000176-009), MSC-05397, NASA/MSC, 11 May 1972.
- "System Safety Program For Systems and Associated Subsystems and Equipment, Requirements for," MIL-STD-882, DOD, 15 July 1969.
- "Systems Safety Guidelines of New Space Operations Concepts," LMSC-A968322, MSFC, Lockheed Missiles and Space Company.
- "Titan IIIC Payload User's Guide," MCR-68-62 Rev. 2, Martin Marietta Corporation, 7 October 1969.